components

2600 Magazine
PO Box 752
Middle Island, NY 11953 U.S.A.
Forwarding and Address Correction Requested

SECOND CLASS POSTAGE
Permit PAID at
East Setauket, N.Y.
11733

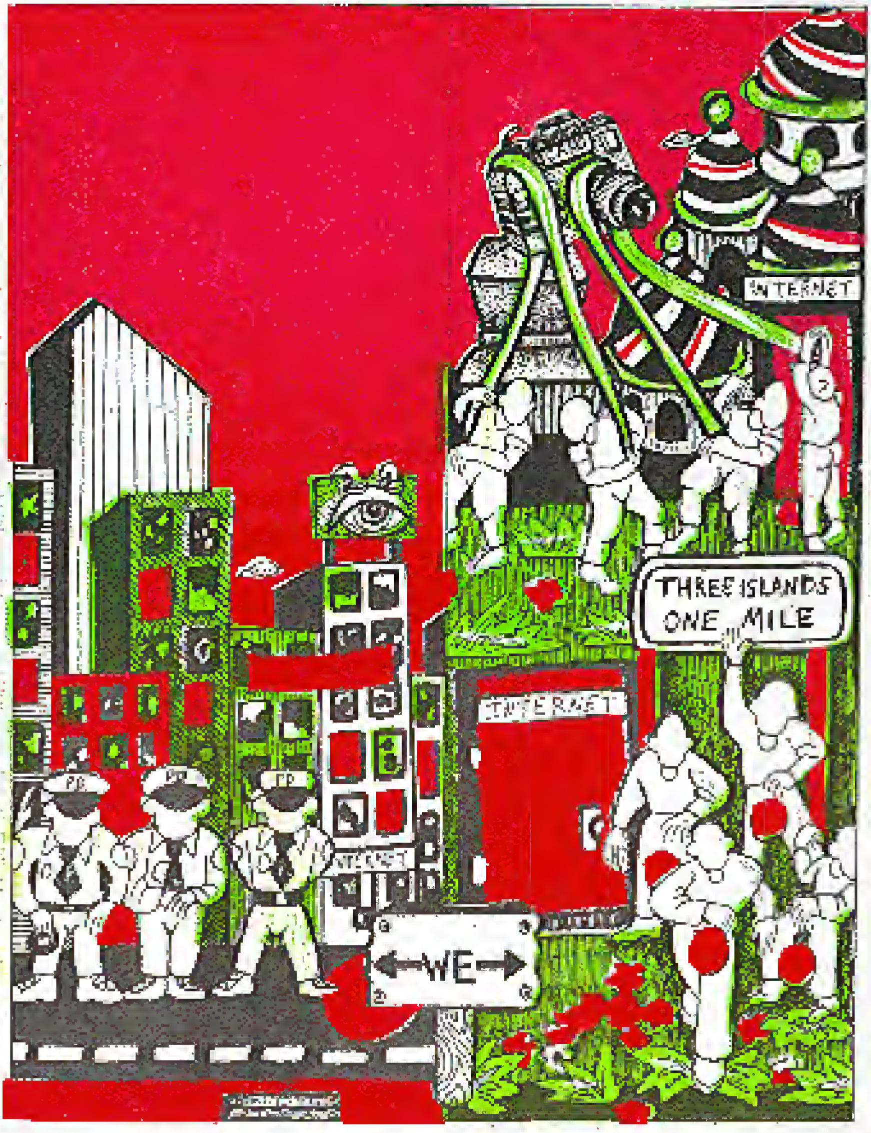
ISSN 0749-3851

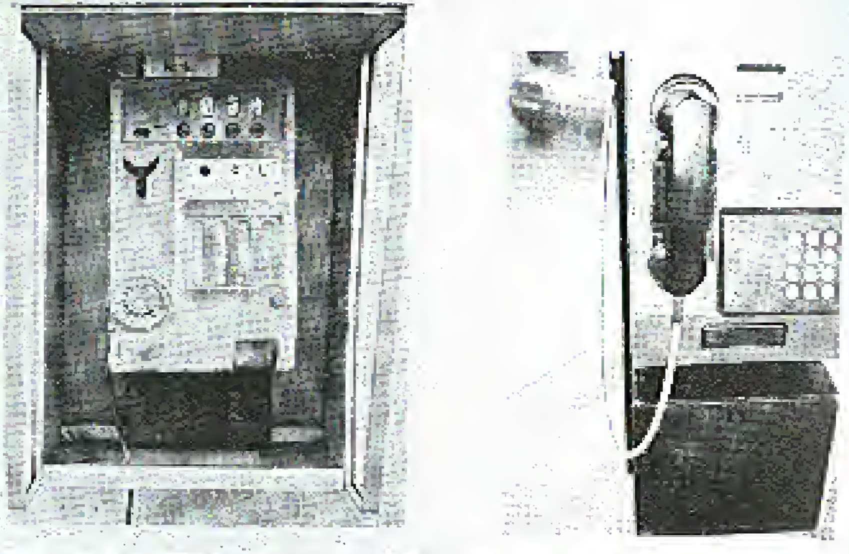
2600

SUPPORT OLYMPIC HACKERS!

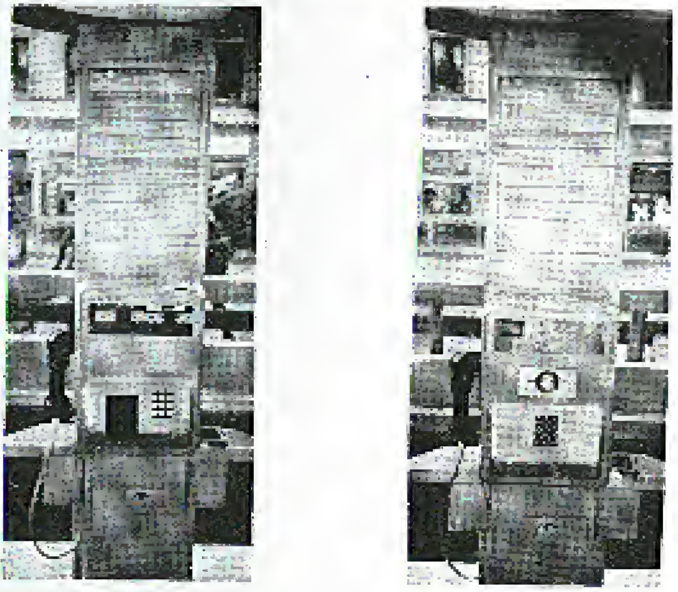
The Hacker Quarterly

VOLUME EIGHT, NUMBER FOUR
WINTER, 1991-92





A vandalized payphone between Casablanca and Marrakech in Morocco. To the right is a money-stealing Moroccan payphone. *Photos by Bernie S.*



Belgian payphones. To the left, one that takes money. To the right, one that takes cards. *Photos by Kingpin*

SEND YOUR PAYPHONE PHOTOS TO: 2600 PAYPHONES, PO BOX 99, MIDDLE ISLAND, NY 11953. IT'S WORTH RISKING YOUR LIFE FOR.

2600 (ISSN 0749-3351) is published quarterly by 2600 Enterprises Inc., 7 Strong's Lane, Setauket, NY 11733. Second class postage permit paid at Setauket, New York.
POSTMASTER: Send address changes to
2600, P.O. Box 752, Middle Island, NY 11953-0752.

Yearly subscription: U.S. and Canada --$21 individual, $50 corporate (U.S. funds).
Overseas -- $30 individual, $65 corporate.
Back issues available for 1984, 1985, 1986, 1987, 1988, 1989, 1990
at $25 per year, $30 per year overseas. Individual issues available
from 1988 on at $6.25 each, $7.50 each overseas.

ADDRESS ALL SUBSCRIPTION CORRESPONDENCE TO:
2600 Subscription Dept., P.O. Box 752, Middle Island, NY 11953-0752.
FOR LETTERS AND ARTICLE SUBMISSIONS, WRITE TO:
2600 Editorial Dept., P.O. Box 99, Middle Island, NY 11953-0099.
INTERNET ADDRESS: 2600@well.sf.ca.us

2600 **Office Line: 516-751-2600,** *2600* **FAX Line: 516-751-2608**

STAFF

Editor-In-Chief
Emmanuel Goldstein

Artwork
Holly Kaufman Spruch

"They are satisfying their own appetite to know something that is not theirs to know."
- Asst. District Attorney Don Ingraham

Writers: Eric Corley, The Devil's Advocate, John Drake, Paul Estev, Mr. French, Bob Hardy, The Infidel, Knight Lightning, Kevin Mitnick, The Plague, Marshall Plann, David Ruderman, Bernie S., Silent Switchman, Scott Skinner, Mr. Upsetter, Dr. Williams, and those who don't fit.

Technical Expertise: Billsf, Rop Gonggrijp, Phiber Optik, Geo. C. Tilyou.

Shout Outs: Andy, Steffen, and future Chaos; Franklin; Toyota Starlet.

50124

2600 CORPORATE HEADQUARTERS

The Atlanta Hacking Center. Our building may not be as big as AT&T's, but we're still able to watch everything they're doing....

Computer Security at the Bureau of Prisons

The following comes from the statement of Richard J. Hankinson, Deputy Inspector General, Office of the Inspector General before the Subcommittee on Government Information, Justice, and Agriculture of the Committee on Government Operations of the U.S. House of Representatives. It concerns computer security at the Bureau of Prisons (BOP) and focuses primarily on the SENTRY system. This took place on September 11, 1991. We thank the reader who forwarded this to us.

The Bureau of Prisons operates three main computer systems:

The SENTRY system is by far the most important, most used, and most sensitive. It is used for management of the 60,000 prisoners, property management, legal reference, and the BOP nationwide electronic mail system. Over 400,000 SENTRY transactions occur every day, and all 19,000 BOP staff members are actual or potential users.

The Batch Transmission System (BTS) is a personal computer (PC) based system that accumulates financial management data at a local institution or BOP office. Data from the PC's is transmitted to the BOP Network Control Center, and then retransmitted to the Justice Management Division (JMD) Data Center in Rockville, Maryland, for processing.

The Federal Prison Point of Sale is a PC based system, networked locally, that is used to record inmate trust fund and commissary transactions at the institution.

Our audit focused on SENTRY, although the other two systems were also tested relative to the security of those two applications. We focused on SENTRY because of the importance of that system to the daily operations of BOP and because of the sensitivity of the data that is stored in and managed by that system.

Our audit work was conducted at BOP Headquarters at the Federal Correctional Center in Sandstone, Minnesota; at the United States Penitentiary in Leavenworth, Kansas; and at the Medical Center in Springfield, Missouri. Additional survey work was also done at the Metropolitan Correctional Center in Chicago, Illinois.

With that background, let me summarize the key deficiencies that we found and what BOP has done in response.

The Network Control Center (NCC) is the critical brain stem that connects data in the field with the mainframe computer in JMD's Rockville Data Center. Both the Batch Transmission System (that handles BOP financial data) and the SENTRY system depend on the effective operation of the NCC. We recommended that a Risk Analysis and Contingency Plan be prepared for this important facility. To its credit, BOP has chosen not to quarrel over whether the NCC meets the technical parameters of the DOJ Order requiring such reviews. Instead, BOP has acknowledged the value of such planning and already has awarded a contract for the work, which is scheduled to be completed in about six months. Once these are completed, they will be reviewed by both our auditors and by the Department's Security Officer.

We found that while BOP uses passwords to limit access to SENTRY terminals, it does not use them to the extent required by DOJ order, nor does it presently provide adequate security or an adequate audit trail. BOP relies on its control of access to offices that contain PC's, and on a terminal-based password (used by all workers in the office or department) to protect against unauthorized access to its computers. This is not adequate. BOP needs to assign a specific password to every individual authorized to access the SENTRY system, to limit the data applications each individual may access and how it may be accessed (i.e., read only, or read and enter data), and it needs to establish password lifetimes (i.e., periodic changes to passwords). By doing so, BOP will tighten control over access to SENTRY, will establish an audit trail that assures individual accountability for transactions performed in SENTRY and that will aid in the detection of unauthorized entries. Although BOP thought it might qualify for an exemption from this requirement, its request was denied on August 20, 1991, and BOP has advised my office that it will implement a password system that conforms to our recommendations by December 31, 1991.

Like some other components in the Department, BOP is delinquent in assuring that background investigations for new hires and reinvestigations every five years for existing employees are conducted on a timely basis. We found that 441 employees in our survey (which totaled 1,684 employees) did not have completed initial background investigations, including 261 employees who had been employed for over a year and 24 who had been employed for over 10 years. An additional 753 employees out of the same sample of 1,684 had not been reinvestigated within five years, as required; 475 of these had not been reinvestigated in over 10 years.

We are satisfied that the Department does indeed have adequate policies in place with regard to computer security. However, much remains to be done. We have directed the Department's components to improve the security of sensitive information processed or stored in departmental computer systems. As a result, JMD and the Offices, Boards, Divisions, and Bureaus are taking steps to further reduce security weaknesses. In July, the Department held an executive briefing regarding computer security awareness for all Department component heads. This executive briefing complements a series of security awareness training sessions already conducted for other employee groups (e.g., managers, and users) throughout the Department in compliance with the Computer Security Act of 1987.

In addition to computer security training, we have taken positive steps on a number of other fronts. These include the following:

Security at the Rockville Data Center. As the Committee is aware, the General Accounting Office identified a number of physical security weaknesses at the Rockville Data Center, ranging from the lack of appropriate alarms to questions regarding access. These have all now been addressed and resolved.

Contingency Planning. With two central, departmental data centers — in Rockville, Maryland and Dallas, Texas — which operate with compatible equipment and the same operating systems, the Department has been well positioned to create an operational contingency backup capacity for its components. We are now in the early stages of making that capacity a reality. This will require a balancing of equipment and operations between the two centers; a reconfiguration of the telecommunications network between Rockville, Dallas, and our field components; and a set of final determinations by each of our components regarding which systems require immediate backup. This process should take about two years and will move the Department of Justice into the front ranks of the government upon completion.

In addition, we have developed a security compliance review program involving departmental components. These reviews cover automated data processing, telecommunications, physical, document, and personnel security. If the component being reviewed has an ADP system designated as "sensitive", the review also covers the implementation of the computer security plan (as required by the Computer Security Act of 1987) and the accuracy of the computer systems security plan. Currently, the Department has 95 systems so designated. As staffing levels and work priorities have permitted, reviews have been conducted since May 1990.

JMD has conducted thirteen computer security reviews in four components (JMD, Tax Division, U.S. Attorneys, Bureau of Prisons). Six reviews were conducted in BOP. (A representative sample of locations was chosen: the Central Office, a regional office, three correctional facilities, and the Denver Training Center.) The BOP has prepared seven computer system security plans covering the seven systems that contain sensitive information. They are: Batch Transmission System, Federal Prison Point of Sale System, SENTRY, Inmate Telephone System, Vehicle Tracking System, BOP Net, and Automated Inmate Management System. It should be noted that four of these systems are operational while three are under development. The SENTRY system was selected for review because it is BOP's primary mission-support system which includes inmate related information and management information sub-systems. SENTRY is a distributive system and serves many diverse users. Over 5,000 SENTRY terminals are now installed nationwide in over 85 correctional facilities in the U.S. and selected BOP Community Program offices, U.S. Parole Commission offices, U.S. Attorney offices, U.S. Probation offices, and U.S. Marshals' offices. On any given day, over 500,000 transactions are processed in response to a variety of requests for information. The reviews validated information in all sections of the computer security plan. As a result of these reviews, the following major weaknesses have been identified: A formal risk analysis has not been conducted; a formal contingency plan has not been developed; user identification and unique passwords are not used; and inadequate computer security awareness training and no formal computer security awareness training for new employees and recurring computer security awareness training for current employees exist.

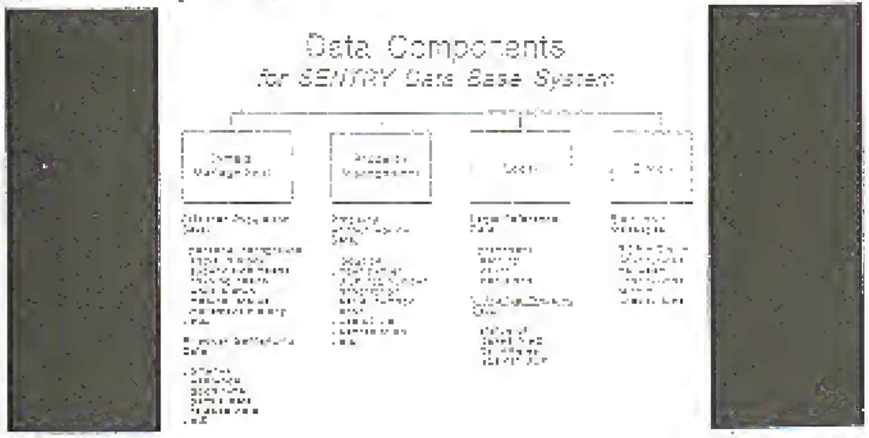
Other findings included concerns regarding interruptible power supply, user session audit trails, and scheduled password changes.

These issues have been presented to the Bureau of Prisons in discussion and will shortly be provided in formal draft for comment.

Earlier I stated that one of the findings of the computer security review was that BOP had not completed its risk analyses. This issue has been addressed in BOP's response. A contract has been signed for the development of a business continuity plan which will include the completion of risk analyses. Another finding of the computer security review was that user identification and unique passwords are not used. In response to our direction, the Bureau has now agreed to provide unique user identification and passwords for SENTRY users by December 31, 1991.

The Bureau has over 20,000 employees who must be trained in accordance with the Computer Security Act. In July, BOP issued guidance which implemented computer security training.

As a final comment, we would only observe that the Department takes its computer security responsibility very seriously. We believe we have an effective program. Only by doing everything within our power to safeguard information can we be reasonably assured that the Department's and the public's interests will continue to be well protected.



Data Components
for SENTRY Data Base System

stuff you should be interested in

Dutch Hacker Raids

by Felipe Rodriquez and Rop Gonggrijp

AMSTERDAM - At 10:30 on the morning of Monday the 27th of January 1992 Dutch police searched the homes of two hackers. In the city of Roosendaal, the parental home of the 21-year old student H.W. was searched and in Nuenen the same happened to the parental home of R.N., a Computer Science engineer, age 25. Both were arrested and taken into custody. At both sites, members of the Amsterdam Police Pilot Team for computer crime were present, alongside local police officers and representatives of the national organization CRI (Criminal Investigations Agency). Both suspects were transported to Amsterdam. The brother of one of the suspects was told the they could receive no visits or mail. The two remained in jail for more than one week.

The Charges

A break-in supposedly occurred at the bronto.geo.vu.nl site at the VU University in Amsterdam. This UNIX system running on a SUN station (Internet Address 130.37.64.3) has been taken off the net at least for the duration of the investigation. What happened to the actual hardware is unknown at this time.

The formal charges are: forgery, racketeering, and vandalism. The police justify the forgery part by claiming that files on the system have been changed. They say the vandalism charge is valid because the system had to be taken off the net for a period of time to investigate the extent of the damage. By pretending to be regular users or even system management the hackers committed racketeering, the police say.

Both suspects, according to the Dutch police, have made a full statement. According to a police spokesman the motive was "fanatical hobbyism." Spokesperson Sloot for the CRI speaks of the "kick of seeing how far you can get."

"Damages"

According to J. Renkema, head of the geophysics faculty at the VU, the university is considering filing a civil lawsuit against the suspects. "The system was contaminated because of their doing and had to be cleaned out. This cost months of labor and 50,000 guilders (about US$ 30,000). Registered users pay for access to the system and these hackers did not. Result: tens of thousands of guilders in damages." Renkema also speaks of a "moral disadvantage." The university lost trust from other sites on the network. Renkema claims the university runs the risk of being expelled from some networks.

Renkema also claims the hackers were discovered almost immediately after the break-in and were monitored at all times. This means all the damages had occurred under the watchful eyes of the supervisors. All this time, no action was taken to kick the hackers off the system. According to Renkema all systems at the VU were protected according to guidelines as laid down by CERT and SurfNet BV (SurfNet is the company that runs most of the inter-university data traffic in The Netherlands).

What Really Happened?

The charge of "adapting system software" could mean that the hackers installed back doors to secure access to the system or to the root level, even if passwords were changed. New versions of telnet, ftp, rlogin, and other programs could have been compiled to log access to the networks.

What really happened is anybody's guess. One point is that even the CRI acknowledges that there were no "bad" intentions on the part of the hackers. They were there to look around and play with the networks.

About Hacking in General

In the past we have warned that new laws against computer crime can only be used against harmless hackers. Against the real computer criminals a law is useless because they will probably remain untraceable. The CRI regularly goes on the record to say that hackers are not the top priority in computer crime investigation. It seems that hackers are an easy target when "something has to be done."

And "something had to be done" - The pressure from especially the U.S. to do something about the "hacking problem" was so huge that it would have been almost humiliating for the Dutch not to respond. It seems as if the arrests are mainly meant to ease the American fear of the overseas hacker-paradise.

A Closer Look at the Charges and Damages

The VU has launched the idea that system security on their system was only needed because of these two hackers. All costs made in relation to system security are billed to the two people that just happened to get in. For people that like to see hacking in terms of analogies: It is like walking into a building full of students, fooling around, and then getting the bill for the new alarm system that they had to install just for you.

Systems security is a normal part of the daily task of every system administrator. Not just because the system has to be protected from break-ins from the outside, but also because the users themselves need to be protected from each other. The "bronto" management has neglected some of their duties, and now they still have to secure their system. This is not damages done, it's work long overdue.

If restoring back-ups costs tens of thousands of guilders, something is terribly wrong at the VU. Every system manager that uses a legal copy of the operating system has a distribution version within easy reach.

"Months of tedious labor following the hackers around in the system." It would have been much easier and cheaper to deny the hackers access to the system directly after they had been discovered. "Moral damages" by break-ins in other systems would have been small. The VU chose to call the police and trace the hackers. The costs of such an operation cannot be billed to the hackers.

Using forgery and racketeering makes one wonder if the OvJ (the District Attorney here) can come up with a better motive than "they did it for kicks." If there is no monetary or material gain involved, it is questionable at best if these allegations will stand up in court.

As far as the vandalism goes: there have been numerous cases of system management overreacting in a case like this. A well trained system-manager can protect a system without making it inaccessible to normal users. Again, the hackers have to pay for the apparent incompetence of system management.

This does not mean that having hackers on your system cannot be a pain. The Internet is a public network and if you cannot protect a system, you should not be on it. This is not just our statement, it is the written policy of many networking organizations. One more metaphor: It's like installing a new phone switch that allows direct dial to all employees. If you get such a system, you will need to tell your employees not to be overly loose-lipped to strangers. It is not the caller's fault if some people can be "hacked." If you tie a cord to the lock and hang it out the mail slot, people will pull it. If these people do damages, you should prosecute them, but not for the costs of walking after them and doing your security right.

Consequences of a Conviction

If these suspects are convicted, the VU has a good chance of winning the civil case. Furthermore, this case is of interest to all other hackers in Holland. Their hobby is suddenly a crime and many hackers will cease to hack. Others will go "underground," which is not beneficial to the positive interaction between hackers and system management or the relative openness in the Dutch computer security world.

Public Systems

If you are not a student at some big university or work for a large corporation, there is no real way for you to get on the Internet. As long as there is no way for some people to connect to the net, there will be people that hack their way in. Whether this is good or bad is besides the point. If there is no freedom to explore, some hackers will become the criminals that government wants them to be.

More AT&T Confusion

Because of a routing error last fall, AT&T mistakenly routed calls made to 800-555-5555 to 900-555-5555. This resulted in people all over the country being billed premium rates for what appeared to be a toll-free call. It's also resulted in an ethical question: should people be billed when they *know* they're being connected to a 900 number by mistake, even though they dialed an 800 number? To us, the answer is pretty clear. AT&T should take the full blame here. It's their network and if they can't manage it properly, customers shouldn't have to pay a penalty. If you're able to find an 800 number that routes to a 900 number, you haven't committed a crime. 800 numbers are toll free and should remain that way. AT&T is now also pushing a product that "translates" 800 numbers to 900 numbers. In other words, a customer can call a company toll-free, ask for a certain service, and then be transferred to a 900 number where the meter starts running. This is an absurd idea that will completely negate the idea of 900 blocking for starters. More importantly, it will confuse consumers even more as to what calls cost money and what calls don't.

Progression

Some good news to report: our friends at The Well are now available on the Internet. This means that many more people will now have access to this electronic meeting ground where freedom of speech and diversity are still held in high regard. It also means that users of The Well will be able to reach out to the Internet, the vast, decentralized network of schools, institutions, and businesses that spans the globe. Unlike those ripoff commercial services, The Well charges a minimal fee ($10 a month and $2 an hour) and is a whole lot more personal. It's also a great environment to learn UNIX and keep in touch with the world via an Internet mailbox. We hope most of our readers take advantage of one of the more positive developments in the high tech world. The Well's online registration number is 415-332-6106 and their new Internet address is 192.132.30.2. Their office number is 415-332-4335.

Regression

A very disturbing incident has occurred in California. On January 20, Robert Thomas, his wife, and their two children were awakened by San Jose police who demanded entry into their home where they proceeded to seize all of their computers and a number of personal effects, including clothing.

At the heart of the matter was a bulletin board, Amateur Action, which stored and distributed adult pictures in the form of GIF files. Thomas did not allow first-time access to the files and he voice-verified all calls. He and his wife took great pains to ensure that the material did not get distributed to anyone underage.

The warrant was for grand theft, bringing obscene matter into the state, and distributing and/or possessing controlled matter of sexual content of persons under 14. Thomas says that none of these accusations apply even remotely to his bulletin board and that he is being persecuted because of its content, viewed as objectionable by some. With such logic, the next step would be to raid the homes of the people who posed in the pictures. Or those of the authors of controversial books.

With the usual obstinance, the authorities are remaining silent and refusing to give anything back. A police officer assured Thomas his equipment would be safe because it would be sitting right on his own desk. In fact, it was later suggested to Thomas that matters would be expedited if he bought the police department a 300 meg hard drive so they could go through the data quicker! Otherwise, they implied, it could drag on for a while.

We're continuing down a very unfriendly road where censorship and raids become commonplace. Hackers were among the first to feel the effects. Now it's spreading to "average American families." Because somebody is suspected of doing something wrong, every bit of high tech equipment on the premises is taken. The most personal of information is now in the hands of the police.

How can one deny that there is a sort of emotional terror in such actions? Imagine if every time you were suspected of anything at all, a vast library of your private thoughts was scanned by the authorities to see what your true feelings really were. That is the ultimate effect of taking people's computers from them. A tremendous amount of information and persona is stored there. Even a hacker, known for wandering where he's told not to go, would feel wrong about going through a personal computer. Faceless entities are one thing. Individuals and families, quite another.

If the mind rape setting doesn't convince you that we're heading straight into a Kafka tale, consider the economic punishment being inflicted here. A family has been deprived of income (several completely legitimate computer-run businesses were being operated from the house) and no charges have even been made. Thomas estimates the value of the seized equipment at $30,000. Thomas' children had their computer taken as well. It contained all of their schoolwork and some games.

If a message is to be understood here, it's that our society is increasingly punishing those of us who do anything even slightly out of the ordinary. There is nothing illegal about running a bulletin board with adult pictures. But not everybody approves. Because of this, a moral judgement quickly turns into a very real form of harassment. After witnessing such actions, how many of us would really have the guts to stand up for free speech?

How many of us can afford to remain silent?

crypt() source

We received quite a few replies to the letter from SJ in our last issue concerning UNIX encryption. Several readers also submitted the source code for the crypt() routine which we are printing below. The following introduction is the most detailed explanation we got. We apologize to you non-math people but sometimes printing this kind of thing is unavoidable.

by Dust
Bern, Switzerland

I followed the discussion about UNIX password encryption with great interest. As I've been studying this subject for quite a long time already, there are some technical remarks I'd like to make about it, because there is still some confusion. About the letter on page 29 of the Autumn 91 issue, I'd like to say that crypt() is not a kernel routine as stated there, but a library function and as such its source is freely available and can be obtained from several anonymous ftp-servers (one is apple.com in the subdirectory pub/ArchiveVol2/4.3bsd-reno/lib/libc/gen/Makefile/crypt.c.Z. (The source file appears at the end of this article.) This routine is the same on all UNIX versions.

It is true, however, that some security experts recommend modifying this call on your site for security reasons, for example, by modifying one of the permutation tables. But this can only be done by recompiling the libraries and it's an action that normally shouldn't be done on UNIX systems, as it makes the system incompatible under certain circumstances (think of NIS, for example). As stated, a possible attacker is better off using such a program offline, for two reasons: First, it won't be discovered as easily, and second, you can implement a much more powerful version of the algorithm. One example of a more efficient implementation is the encryption used in the "Cracker" program, a password hacking program written for system administrators to check the quality of user-chosen passwords. I also implemented such a program and reach even a slightly better thruput: the C-version reaches about 900 encryptions on a sparcstation 2, and the 68000- assembler version reaches 72 per second on an Atari-ST (and probably also on an Amiga). I won't publish the source codes here, but I think there's no problem in explaining the main mathematical ideas of improving the algorithm. Those ideas are taken out of the paper "An Application of a Fast Data Encryption Standard Implementation" by Matt Bishop, Dartmouth College & RIACS. I'm aware this paper isn't officially available and won't copy it in full extent, but as far as I know there's no law against explaining the ideas on a mathematical basis.

First I'll explain the DES algorithm itself (which is part of crypt), but I won't include the actual tables, which you find in the source code. About notation, ^ means bitwise xor. DES itself consists of permutations written as P_...(), expansions written as E_...(), and substitutions written as S_...(). Permutations exchange bit positions of a given bit string in a reversible way, expansions do the same but use several bit-positions several times (so the output is wider) or not at all (so the output is smaller, actually a contraction), and substitutions substitute chunks of bit-substrings according to a fix table.

DES takes a clear text (64 bits) and a key K (64 bits) as input. The key is used to calculate 16 intermediate keys in the following way: Using an expansion E_PC1(K), the first intermediate key K[0] is calculated (E_PC1 is a contraction, it only uses 56 of the 64 bits; the remaining ones are considered as parity-bits). Then the following ones are calculated as K[i]=P_LSH_i(K[i-1]), so just a special permutation (actually a left-shift) is applied to the previous intermediate key. Finally, the subkeys k[i] are calculated as k[i]=P_PC2(K[i]), by applying a further permutation to the intermediate keys. Note that P_PC2 contracts the 56 bit input to 48 bits, so each k[i] is 48 bits wide.

Then the clear text m is encrypted: Using an initial permutation, we get a 64 bit wide output T[0] = P_IP(M). Those are divided into two halves l[0] and r[0], each 32 bits wide.The next 16 steps are the same, the output of each being used as the input for its successor. For rounds i=0,...,15:

(1) l[i+1] = r[i]
(2) r[i+1] = l[i] ^ P_P(S_S(E_E(r[i]) ^ k[i]))

In this equation, E_E expands the 32-bit wide r[i] to 48 bits, S_S substitute the 8 6-bit-chunks by 8 4-bit-chunks using 8 different but given tables, producing 32 bits of output, which are permuted by P (also giving 32 bits output). Finally, the two halves l[16] and r[16] are concatenated and the reverse initial permutation applied to it, which gives the result P_FP(r[16]l[16]).

Now, the main mathematical improvement

consists in applying E_E to both sides of equations (1) and (2):

E_E(l[i+1]) = E_E(r[i])

E_E(r[i+1]) = E_E(l[i] ^ P_P(S_S(E_E(r[i]) ^ k[i])))

As you see, you apply a bit permutation on a bitwise xor; you can as well apply the E_E permutation to both sides of the xor first, and afterwards xor them, because xor doesn't change the bit positions, giving

E_E(r[i+1]) = E_E(l[i]) ^ E_E(P_P(S_S(E_E(r[i]) ^ k[i])))

Now we'll write L[i] instead of E_E(l[i]) and R[i] instead of E_E(r[i]), and we use the operator F(..) = E_E(P_P(S_S(..))), giving

L[i+1] = R[i]

R[i+1] = L[i] ^ F(R[i] ^ k[i])

and thus, always using the above two equations

L[i+2] = R[i+1] = L[i] ^ F(R[i] ^ k[i])

R[i+2] = L[i+1] ^ F(R[i+1] ^ k[i+1])

  = R[i] ^ F(L[i] ^ F(R[i] ^ k[i]) ^ k[i+1])

  = R[i] ^ F(L[i+2] ^ k[i+1])

so, as a result of the improvement, we get

L[i+2] = L[i] ^ F(R[i] ^ k[i])

R[i+2] = R[i] ^ F(L[i+2] ^ k[i+1])

(using above result) we only have to use them eight times, as only even indices appear; however, we still have to apply an operation of the type x ^ F(y ^ z) 16 times. But the operation "F", which actually combines S-substitutions, P-permutation, and E-permutation, can be performed by constructing a table, input and output being 48 bits wide. Note that you can't implement such a big table in one piece; you can, however, use four tables, each covering 12 bits of input (note that the substitutions take 6-bit chunks, so you must partition to parts divisible by 6). Each of those tables is indexed by a 12-bit input (4096 entries), giving a 48-bit result. You use those tables by separating the four 12-bit parts, for each calculating the result by using the tables, and finally xor the four results. For efficiency, I recommend stuffing the 48 bits to 64 bits in the way that each 12-bit sub-part is aligned to 16 bits (this allows faster access to the subparts, as rotating by 16 bits can often be performed by a special command, for example "swap" on a 68000). This way, each of the 4096 entries uses 8 bytes, giving a size of 32K; all four tables then need 128K of memory.

Note, of course, that you must also modify P_IP and P_FP to add the E-permutation and take it back in the end, as in the main loop, you always calculate with L[i] and R[i] instead of l[i] and r[i]; but there's nothing new about it, and it is easy to realize it yourself. Also note that you can make things a bit faster by combining P_PC2, P_LSH, and P_PC1; but the main time of the algorithm is eaten away by the main loop, this one is performed 400 times during a crypt() encryption.

That was the mathematical part. Now considering UNIX's crypt(): it works the following way: using a 12 bit salt code, the E-permutation is modified by swapping some entries. Then the password is taken as key, which encrypts a block of 64 0-bits according to DES 25 times (thus the above operation is executed 25*16 = 400 times). Note that you can leave away the intermediate P_IP and P_FP permutations, as they are inverse operations. Also note that you need to calculate the sub-keys only one time (they are re-used). I'm using the following procedure to check a password: out of the encrypted password; I extract the salt-code (the first 2 characters), which isn't encrypted. Based on it, I build the modified E_E table and then the F-table because F depends on E_E. This takes a lot of time, because it fills 128K of memory (it eats nearly a second in my implementation), but this doesn't count much, because you only need to do it once; afterwards you probably use the encryption thousands of times using the same salt, depending on the size of your dictionary. Also think of the fact that, to be efficient, you should check all encrypted passwords with the same salt-code within a password file at the same time, which can be done by sorting the password file according to their salt.

That was all about it. Note that it's best to implement it in assembler. The C-version is much slower, mainly because of the lack of a command to rotate a bit string (C supports only shifting), and because you're unable to express an action like "swap" (which exchanges low and high 16 bits of a 32-bit word) in an efficient way. However, a C-version is easier to implement on a machine with an unknown hardware (unfortunately I don't know Sparc assembler...).

```
#if defined(LIBC_SCCS) && !defined(lint)
static char sccsid[] = "@(#)crypt.c   5.3 (Berkeley) 5/11/90";
#endif LIBC_SCCS and not lint

/*
 * This program implements the
 * Proposed Federal Information Processing
 *  Data Encryption Standard.
 * See Federal Register, March 17, 1975 (40FR12134)
 */

/*
 * Initial permutation,
 */
static          char            IP[] = {
                58,50,42,34,26,18,10, 2,
                60,52,44,36,28,20,12, 4,
                62,54,46,38,30,22,14, 6,
                64,56,48,40,32,24,16, 8,
                57,49,41,33,25,17, 9, 1,
                59,51,43,35,27,19,11, 3,
                61,53,45,37,29,21,13, 5,
                63,55,47,39,31,23,15, 7,
};

/*
 * Final permutation, FP = IP^(-1)
 */
static          char            FP[] = {
                40, 8,48,16,56,24,64,32,
                39, 7,47,15,55,23,63,31,
                38, 6,46,14,54,22,62,30,
                37, 5,45,13,53,21,61,29,
                36, 4,44,12,52,20,60,28,
                35, 3,43,11,51,19,59,27,
                34, 2,42,10,50,18,58,26,
                33, 1,41, 9,49,17,57,25,
};

/*
 * Permuted-choice 1 from the key bits
 * to yield C and D.
 * Note that bits 8,16... are left out:
 * They are intended for a parity check.
 */
static          char            PC1_C[] = {
                57,49,41,33,25,17, 9,
                 1,58,50,42,34,26,18,
                10, 2,59,51,43,35,27,
                19,11, 3,60,52,44,36,
};

static          char            PC1_D[] = {
                63,55,47,39,31,23,15,
                 7,62,54,46,38,30,22,
                14, 6,61,53,45,37,29,
                21,13, 5,28,20,12, 4,
};

/*
 * Sequence of shifts used for the key schedule.
 */
static          char            shifts[] = {
                1,1,2,2,2,2,2,2,1,2,2,2,2,2,2,1,
};

/*
 * Permuted-choice 2, to pick out the bits from
 * the CD array that generate the key schedule.
 */
static          char            PC2_C[] = {
                14,17,11,24, 1, 5,
                 3,28,15, 6,21,10,
                23,19,12, 4,26, 8,
                16, 7,27,20,13, 2,
};

static          char            PC2_D[] = {
                41,52,31,37,47,55,
                30,40,51,45,33,48,
                44,49,39,56,34,53,
                46,42,50,36,29,32,
};

/*
 * The C and D arrays used to calculate the key schedule.
 */

static          char            C[28];
static          char            D[28];
/*
 * The key schedule.
 * Generated from the key.
 */
static          char            KS[16][48];

/*
 * The E bit-selection table.
 */
static          char            E[48];
static          char            e[] = {
                32, 1, 2, 3, 4, 5,
                 4, 5, 6, 7, 8, 9,
                 8, 9,10,11,12,13,
                12,13,14,15,16,17,
                16,17,18,19,20,21,
                20,21,22,23,24,25,
                24,25,26,27,28,29,
                28,29,30,31,32, 1,
};

/*
 * Set up the key schedule from the key.
 */

setkey(key)
char *key;
{
                register i, j, k;
                int t;

                /*
                 * First, generate C and D by permuting
                 * the key.  The low order bit of each
                 * 8-bit char is not used, so C and D are only 28
                 * bits apiece.
                 */
                for (i=0; i<28; i++) {
                                C[i] = key[PC1_C[i]-1];
                                D[i] = key[PC1_D[i]-1];
                }
                /*
                 * To generate Ki, rotate C and D according
                 * to schedule and pick up a permutation
                 * using PC2.
                 */
                for (i=0; i<16; i++) {
                                /*
                                 * rotate.
                                 */
                                for (k=0; k<shifts[i]; k++) {
                                                t = C[0];
                                                for (j=0; j<28-1; j++)
                                                    C[j] = C[j+1];
                                                C[27] = t;
                                                t = D[0];
                                                for (j=0; j<28-1; j++)
                                                    D[j] = D[j+1];
                                                D[27] = t;
                                }
                                /*
                                 * get Ki. Note C and D are concatenated.
                                 */
                                for (j=0; j<24; j++) {
                                        KS[i][j] = C[PC2_C[j]-1];
                                        KS[i][j+24] = D[PC2_D[j]-28-1];
                                }
                }
```

```
        for(i=0;i<48;i++)
                E[i] = e[i];
}

/*
 * The 8 selection functions.
 * For some reason, they give a 0-origin
 * index, unlike everything else.
 */
static  char    S[8][64] = {
        14, 4,13, 1, 2,15,11, 8, 3,10, 6,12, 5, 9, 0, 7,
         0,15, 7, 4,14, 2,13, 1,10, 6,12,11, 9, 5, 3, 8,
         4, 1,14, 8,13, 6, 2,11,15,12, 9, 7, 3,10, 5, 0,
        15,12, 8, 2, 4, 9, 1, 7, 5,11, 3,14,10, 0, 6,13,

        15, 1, 8,14, 6,11, 3, 4, 9, 7, 2,13,12, 0, 5,10,
         3,13, 4, 7,15, 2, 8,14,12, 0, 1,10, 6, 9,11, 5,
         0,14, 7,11,10, 4,13, 1, 5, 8,12, 6, 9, 3, 2,15,
        13, 8,10, 1, 3,15, 4, 2,11, 6, 7,12, 0, 5,14, 9,

        10, 0, 9,14, 6, 3,15, 5, 1,13,12, 7,11, 4, 2, 8,
        13, 7, 0, 9, 3, 4, 6,10, 2, 8, 5,14,12,11,15, 1,
        13, 6, 4, 9, 8,15, 3, 0,11, 1, 2,12, 5,10,14, 7,
         1,10,13, 0, 6, 9, 8, 7, 4,15,14, 3,11, 5, 2,12,

         7,13,14, 3, 0, 6, 9,10, 1, 2, 8, 5,11,12, 4,15,
        13, 8,11, 5, 6,15, 0, 3, 4, 7, 2,12, 1,10,14, 9,
        10, 6, 9, 0,12,11, 7,13,15, 1, 3,14, 5, 2, 8, 4,
         3,15, 0, 6,10, 1,13, 8, 9, 4, 5,11,12, 7, 2,14,

         2,12, 4, 1, 7,10,11, 6, 8, 5, 3,15,13, 0,14, 9,
        14,11, 2,12, 4, 7,13, 1, 5, 0,15,10, 3, 9, 8, 6,
         4, 2, 1,11,10,13, 7, 8,15, 9,12, 5, 6, 3, 0,14,
        11, 8,12, 7, 1,14, 2,13, 6,15, 0, 9,10, 4, 5, 3,

        12, 1,10,15, 9, 2, 6, 8, 0,13, 3, 4,14, 7, 5,11,
        10,15, 4, 2, 7,12, 9, 5, 6, 1,13,14, 0,11, 3, 8,
         9,14,15, 5, 2, 8,12, 3, 7, 0, 4,10, 1,13,11, 6,
         4, 3, 2,12, 9, 5,15,10,11,14, 1, 7, 6, 0, 8,13,

         4,11, 2,14,15, 0, 8,13, 3,12, 9, 7, 5,10, 6, 1,
        13, 0,11, 7, 4, 9, 1,10,14, 3, 5,12, 2,15, 8, 6,
         1, 4,11,13,12, 3, 7,14,10,15, 6, 8, 0, 5, 9, 2,
         6,11,13, 8, 1, 4,10, 7, 9, 5, 0,15,14, 2, 3,12,

        13,  2, 8, 4, 6,15,11, 1,10, 9, 3,14, 5, 0,12, 7,
         1,15,13, 8,10, 3, 7, 4,12, 5, 6,11, 0,14, 9, 2,
         7,11, 4, 1, 9,12,14, 2, 0, 6,10,13,15, 3, 5, 8,
         2, 1,14, 7, 4,10, 8,13,15,12, 9, 0, 3, 5, 6,11,
};

/*
 * P is a permutation on the selected combination
 * of the current L and key.
 */
static  char    P[] = {
        16, 7,20,21,
        29,12,28,17,
         1,15,23,26,
         5,18,31,10,
         2, 8,24,14,
        32,27, 3, 9,
        19,13,30, 6,
        22,11, 4,25,
};

/*
 * The current block, divided into 2 halves.
 */
static  char    L[64], *R = L+32;
static  char    tempL[32];
static  char    f[32];

/*
 * The combination of the key and the input, before selection.
 */
static  char    preS[48];

/*
 * The payoff: encrypt a block.
 */

encrypt(block, edflag)
char *block;
{
        int i, ii;
        register t, j, k;

        /*
         * First, permute the bits in the input
         */
        for (j=0; j<64; j++)
                L[j] = block[IP[j]-1];
        /*
         * Perform an encryption operation 16 times.
         */
        for (ii=0; ii<16; ii++) {
                /*
                 * Set direction
                 */
                if (edflag)
                        i = 15-ii;
                else
                        i = ii;
                /*
                 * Save the R array,
                 * which will be the new L.
                 */
                for (j=0; j<32; j++)
                        tempL[j] = R[j];
                /*
                 * Expand R to 48 bits using
                 * the E selector;
                 * exclusive-or with the
                 * current key bits.
                 */
                for (j=0; j<48; j++)
                    preS[j] = R[E[j]-1] ^ KS[i][j];
                /*
                 * The pre-select bits are
                 * now considered
                 * in 8 groups of 6 bits each.
                 * The 8 selection functions
                 * map these
                 * 6-bit quantities into
                 * 4-bit quantities
                 * and the results permuted
                 * to make an f(R, K).
                 * The indexing into the
                 * selection functions
                 * is peculiar; it could
                 * be simplified by
                 * rewriting the tables.
                 */
                for (j=0; j<8; j++) {
                    t = 6*j;
                    k = S[j][(preS[t+0]<<5)+
                            (preS[t+1]<<3)+
                            (preS[t+2]<<2)+
                            (preS[t+3]<<1)+
                            (preS[t+4]<<0)+
                            (preS[t+5]<<4)];
                    t = 4*j;
                    f[t+0] = (k>>3)&01;
                    f[t+1] = (k>>2)&01;
                    f[t+2] = (k>>1)&01;
                    f[t+3] = (k>>0)&01;
                }
                /*
                 * The new R is L ^ f(R, K).
                 * The f here has to be
                 * permuted first, though.
                 */
                for (j=0; j<32; j++)
                    R[j] = L[j] ^ f[P[j]-1];
                /*
                 * Finally, the new L
                 * (the original R)
                 * is copied back.
                 */
                for (j=0; j<32; j++)
                    L[j] = tempL[j];
        }
        /*
         * The output L and R are reversed.
         */
        for (j=0; j<32; j++) {
                t = L[j];
                L[j] = R[j];
                R[j] = t;
        }
        /*
         * The final output
         * gets the inverse permutation
         * of the very original.
         */
        for (j=0; j<64; j++)
                block[j] = L[FP[j]-1];
}

char *
crypt(pw,salt)
char *pw;
char *salt;
{
        register i, j, c;
        int temp;
        static char block[66], iobuf[16];

        for(i=0; i<66; i++)
                block[i] = 0;
        for(i=0; (c= *pw) && i<64; pw++){
                for(j=0; j<7; j++, i++)
                    block[i] = (c>>(6-j)) & 01;
                i++;
        }

        setkey(block);

        for(i=0; i<66; i++)
                block[i] = 0;

        for(i=0;i<2;i++){
                c = *salt++;
                iobuf[i] = c;
                if(c>'Z') c -= 6;
                if(c>'9') c -= 7;
                c -= '.';
                for(j=0;j<6;j++){
                    if((c>>j) & 01){
                        temp = E[6*i+j];
                        E[6*i+j] = E[6*i+j+24];
                        E[6*i+j+24] = temp;
                    }
                }
        }

        for(i=0; i<25; i++)
                encrypt(block,0);

        for(i=0; i<11; i++){
                c = 0;
                for(j=0; j<6; j++){
                    c <<= 1;
                    c |= block[6*i+j];
                }
                c += '.';
                if(c>'9') c += 7;
                if(c>'Z') c += 6;
                iobuf[i+2] = c;
        }
        iobuf[i+2] = 0;
        if(iobuf[1]==0)
                iobuf[1] = iobuf[0];
        return(iobuf);
}
```

Birth of a Low Technology Hacker

by The Roving Eye

I hope by this article that you can see how a hacker is born in a totally different culture than yours.

I was born on the coldest day in North India in 46 years, though I do not think that that was the true birth of the hacker that I call myself. I was born into a poor family and in place of the usual inclination for crime that goes with such a background, I was instead given three things: a permanent dark tan, a curious brain, and a desire to beat the system with that curious brain. It was this combination of the last two that gave me the hacker spirit that I share with you, whereas everything else about me is very different. All my life I have thought of ways to defeat authority and power, but always within the framework of their own system. When I was little I always found loopholes in my parents' statements and got away with whatever I wanted. At the age of eight I was already experimenting with radios, trying to make magnets and so on. When I was ten I learned to read circuit diagrams and I started making my own ten bit binary adding machine using only simple switches, small bulbs, and a battery. My parents were impressed and so I got my first book allowance. For the equivalent of a dollar a month, I could get whatever Soviet books I wanted.

But that was not enough for me. I started my own library with books that my older friends donated, and by twelve I had a catalogued library of four hundred books. I now found that because of my good knowledge of things, I could often get away with all sorts of things. I soon learned to manipulate the water meter so that it would not move at all and thus the company would charge us by the flat rate. By experimenting I got the electric meter to run slowly when I stuck a magnet to the side. The technology was so simple that even I could defeat it at the age of thirteen.

But India is a low tech country. I had not seen a credit card or a touchtone phone or even been to an airport before I came to the United States. So I had to find other avenues for my talents.

At thirteen my parents were sick of my tricks and sent me away to boarding school. It was there that I found the real inspiration. First and foremost I defeated the system to switch the lights out at lights out time. By putting a switch in parallel, I could switch the lights on from inside the dormitory, after the teacher had put them out from outside. My father used to work in research then. Using the excuse of a science project, I got him to get me a photocell. Using this, we put a trip on the main dorm door to warn us when the master came. Finally, we put a power relay to the lights with input from the radio, and we had our own mini disco. Soon I was unstoppable.

One adventure led to another. The school had a few BBC Acorn Electron computers which we used to "become familiar with computers." Actually they were no good for this or any purpose. The thing we did use them for was to get to our billing records. The student computer room was separated from the school computer room by only a grill, to save the air conditioning costs. One night two friends and I managed to remove a section of this grill and hook up an IBM keyboard and monitor to the school system. Then we placed this keyboard as that of one of the Acorn Electrons, so no one would suspect anything. Even when a teacher walked by, he only commended us on our efforts to educate ourselves.

It was not long before we had used the accountant's daughter's name as the password to break in. We did not change anything, though, but the thrill of being able to was so great. Soon my friend was able to acquire a "keyboard tap." This is a great device that lets you put two keyboards and monitors on a computer, and switch between them by flipping a switch. I am really surprised that in the mass of tangled wires that only the fellow from the company understood, no one ever found the tap device for a full semester.

My friend was rich and had a computer at home, and he did all the work, and my job was merely to be a lookout, keep trying passwords, or something like that. I had no clue as to what my friends were doing most of the time, because they already knew about all this stuff, and they never had time to explain. But I tried to learn the system on my own. Whenever I had time, I would be back at the computer. Not, as I look back now, that it did much good. Without the manuals I just wasted most of my time.

You must understand that in our sort of technological setting, this was quite an achievement for all of us. We looked at our grades, saw other people's reports and so on quite at will, all the time right under the nose of the people. And because of the thrill the whole thing gave me, a true hacker was born.

Since then I managed to tap phones, and even hook up my own homemade intercom to the new internal phone system that the school got when some big alumnus donated us some money. The crowning glory arrived when I came to America. Not fully realizing what the potential of someone with a need and zeal can achieve, the corporations are quite lax in this direction. But I have found that the best answers to beating the system are the simplest. The "phone does not work correctly" method of fooling the operator, especially with my accent, has been the most effective for me. And as for breaking into the systems of our school, anyone with a bit of sweet-talking skills can find out anything. Not to mention the advantages one can reap by being aware of the tremendous amounts of money, things, information, and so on that Uncle Sam and Cousin Big Blue or the Fed are ready to give out for free, when presented with the right story. I cannot lay claim to very great technical knowledge or achievements. "But the spirit is the thing," my mother says. So I guess as a low tech hacker I have definitely made my mark.

My life has become quite different as a result of seeing my friends access our billing accounts. Being a socially insecure person, I have built a digital wall against society. By being sort of apart from them, I am able to understand people much better. Thus I am now trying to hack the ultimate machine: the human brain. I have found that most often people are much more vulnerable to manipulation in undesired ways than machines. Though I must admit that toying around with the mega-monsters of this technocratic society is a lot more fun...

mobile frequencies

by Esper

Cellular phone phreaking is an area that remains, for the most part, untapped (no pun intended). Let me rephrase that - it remains, for the most part, *unreported* within the hacker/-phreak community. To many aspiring phreaks and seasoned veterans, cellular phone systems are pretty much uncharted waters, ready to be sailed. Unfortunately, those who may have discovered new ways to utilize cellular phones are being tight-lipped about it, or are just researching it a little further before coming out with ways to do it and telling others, such as in *2600*. Hopefully, we will see some articles about this in future issues. In the past, there was one such article concerning *mobile* phones (not to be confused with cellular), which leads into something creative. Bear with me.

Now for a trip down memory lane. For those who are fortunate enough to keep up with back issues, you might remember there was an article some time ago detailing mobile phone theory and construction by The Researcher (*2600 Magazine*, Vol. 3, Number 4, April 1986). Details were given on how to construct one using a cassette tape recorder, radio scanner, a low-power transmitter, and a mobile phone dialer (build your own). In the article, the author suggests building a Wein-Bridge oscillator to generate red box tones. For this, it might be easier to build a red box from a Radio Shack tone dialer (most recent conversion is highlighted in the Autumn 1991 issue of *2600*). I won't get into the gory details of the article, so you might have to find a copy of it somewhere or buy the back issues. Again, bear with me.

In the mobile phone article, it tells how you should set the transmitter to the corresponding mobile frequency, send the ID sequence that you taped with the cassette recorder, and use the dialer to call "one of those special 800 numbers and whistle off with 2600 hertz; then MF to anywhere in the world." While I'm not sure how easily Ma Bell can nail someone blue boxing over a mobile phone, I and many others know how bad an idea of blue boxing over regular lines can be. In any case, this is an idea for phreakers and hackers alike.

Trouble is, finding mobile phone frequencies is kind of a hit and miss deal with a scanner. There are lots of bands to cover, and one might only have a vague idea as to what frequencies are where. If you manage to hit upon an unused frequency, you'll hear that all-too-familiar 2600 hertz tone heading down the line until someone makes a call. Then you'll hear the ID sequence, the number being dialed, and lo and behold! You'll hear a call! To make your lives a little easier, here's a list of mobile phone channels used by the phone companies in major cities across the nation. If there's more than one frequency used in one three-digit number (I've seen 8-9), I'll list them like this: **City:** XXX (yyy,yyy,yyy,yyy,yyy) MHz. XXX.yyy would thus be a valid frequency for that city.

Albuquerque: 152. (510, 570, 630, 750, 810)

Atlanta: 152. (510, 540, 600, 630, 660, 690, 750, 810)

Baltimore: 152. (510, 630, 750, 810), 454. (400, 500)

Boston: 152. (510, 540, 600, 660, 780), 454. (524, 475, 500, 525, 550, 600)

Chicago: 152. (510, 570, 630, 690, 720, 750, 780, 180), 454. (375, 400, 425, 450, 475, 500, 525, 550, 575, 600, 625, 650)

Cincinnati: 152. (510, 630, 750)

Cleveland: 152. (510, 630, 690, 750), 454.400

Dallas: 152. (510, 630, 690, 750, 810), 454. (400, 475, 550, 600, 525, 650)

Denver: 152. (510, 540, 600, 630, 690, 750, 780, 810), 454. (375, 400, 425, 450, 475, 500, 525, 550, 575, 600, 625, 650)

Detroit: 152. (570, 600, 630, 690, 730), 454. (375, 475, 525, 575, 625)

Houston: 152. (510, 630, 720, 750), 454. (400, 425, 450, 475, 500, 550, 600, 650)

Indianapolis: 152. (510, 540, 630, 690, 750, 810), 454. (375, 400, 425, 475, 500, 525, 550, 600)

Kansas City: 152. (510, 540, 630, 690, 750, 780), 454. (375, 425, 450, 475, 550, 650)

Las Vegas: 152. (510, 540, 570, 630, 690, 720, 750, 780), 454. (375, 425, 450, 500, 550, 575, 625)

Miami: 152. (510, 570, 600, 630, 660, 720, 750, 780), 454. (375, 400, 425, 450, 500, 550, 600)

Milwaukee: 152. (510, 570, 600, 630, 720, 780), 454. (400, 475, 600)

Minneapolis/St. Paul: 152. (510, 570, 630, 690, 780, 810), 454. (375, 450, 475, 525, 600, 625)

Nashville: 152. (510, 570, 630, 690, 780, 810), 454. (375, 450, 475, 525, 600, 625)

Newark, NJ: 152. (540, 750, 810), 454. (425, 475, 575)

New Orleans: 152. (510, 630, 690, 810)

New York City: 152. (510, 570, 630, 690, 720, 780), 454. (375, 450, 525, 550, 625, 650)

Oklahoma City: 152. (510, 540, 630, 660, 720, 750, 580, 810), 454. (375, 400, 425, 475, 500, 600, 650)

Philadelphia: 152. (510, 540, 630, 690, 750, 810), 454. (400, 425, 475, 500, 550, 575, 600, 650)

Phoenix: 152. (540, 570, 600, 630, 660, 720, 750, 780, 810)

Pittsburgh: 152. (510, 630, 690, 750), 454. (375, 400, 425, 475)

St. Louis: 152. (510, 570, 630, 660, 690, 750), 454. (375, 400, 425, 450, 550)

Salt Lake City: 152. (510, 570, 630, 690, 750, 810)

San Diego: 152. (510, 570, 630, 690, 810), 454.550

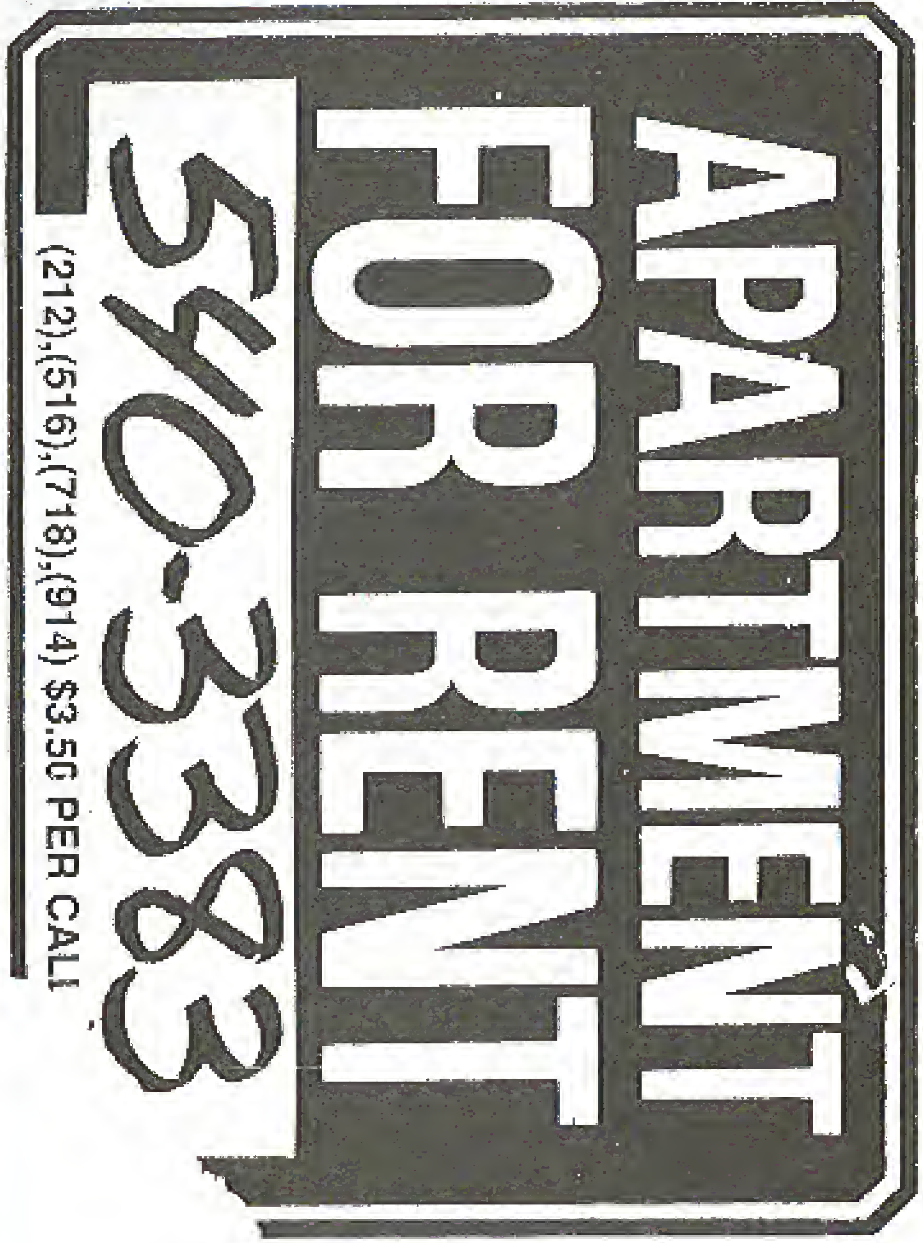
San Francisco: 152. (510, 540, 630), 454.550

Seattle: 152. (510, 540, 630, 660, 690), 454. (375, 450, 500)

Washington: 152. (510, 600, 630, 690, 720, 750, 780, 810), 454. (375, 425, 475, 525, 550, 575, 625, 650)

There are some other frequencies that don't fall under the normal 152 or 454 MHz band. Some can be found in the 35 MHz band and, from what I've seen and heard, they aren't used much. This is either good or bad. It's good because it's almost always free of use, but bad for the same reason. In order to hide among the masses, it might be better to stick to the 152 or 454 band. I haven't had the opportunity to build these phones or test them, but as food for thought and creative processes, I hope I've whetted some appetites. And, if any of what I've proposed pans out, write and tell us, schematics and all. Knowledge is power. Even if you have no intention of building the mobile phone and using the frequencies listed above, they are always fun to give a listen to. One time I caught a prominent real estate mogul who is in financial dire straits (I can't say who; besides, Donald would never forgive me) call one woman and say he was working late and wouldn't be home for quite a while. He then called another woman and told her he'd be over at 6:30. Who knows what you'll hear?

One final note: if you like what you hear, you might want to pick up the police/fire radio frequency book for your state while you're in Radio Shack for your tone dialer. Keep an eye on Big Brother. Hell, they're probably keeping an eye on you! Happy hunting!



BY PUTTING THESE SIGNS ON TELEPHONE POLES, THE PEOPLE BEHIND THIS SCAM STAND A GOOD CHANCE OF SNAGGING A FEW UNSUSPECTING CLODS WHO CAN'T READ THE FINE PRINT AS THEY DRIVE BY.

Simplex Update and Corrections

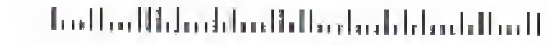
Four superfluous codes were printed in the list of possible Simplex lock combinations on page 12 of the Autumn 1991 issue. The codes (51), (52), (53), and (54) are unnecessary because they are already included in the list under a different guise. The code (51), for instance, is the same as (15) because the pushbuttons are pressed together. Subsequently, this brings the total number of possible combinations down from 1085 to 1081.

An error was also made on page 45 regarding the total number of Group D combinations. The number should be 541, not 451.

We decided to follow our own advice on page 11 and record the Simplex codes onto cassette. Using speech synthesis software on an Amiga 2000, we programmed the machine to do all the dirty work. The speaking rate of the voice as well as the pauses between the codes were carefully adjusted so that the approximate running time is 75 minutes. In the time that it takes you to listen to this cassette, you could be in any Simplex lock.

If you'd like to see just how easy it really is, send us $7.50 and we'll send you a cassette with all of the codes! The address is 2600, PO Box 752, Middle Island, NY 11953.

USPS Hacking Corrections



The correct POSTNET for 11953-0752, our zip code.

As many of you wrote to tell us, the graphic POSTNET examples that appear on pages 32 and 36 are incorrect.

To prevent this heinous error from ever occurring again, we now use one of two programs to print POSTNET's. One program is in BASIC while the other is in C. Both ask for a five or nine digit ZIP code as input and then print an equivalent POSTNET. Both are printed in this issue.

A final correction: FIM's are not necessarily "six-line bar codes" as claimed on pages 32-33. They can have anywhere from five to seven bars depending on the type.

POSTNET PROGRAMS

BASIC VERSION

```
1 ' Jiffy-Ya Zipcoder Program by Marshall Plann
10 WIDTH "lpt1:",255
20 K2 = 6 ' Thickness of the stripes
30 K1 = 5 ' Thickness of the gaps
40 SUM = 0
50 PRINT "Enter Zip Code : ";
60 INPUT A$ : L = LEN(A$)
70 ' Initialize Printer and print first long bar
80 GOSUB 250 : GOSUB 370
90 ' process each digit
100 FOR I = 1 TO L : Z$ = MID$(A$,I,1) : GOSUB 190 :
     NEXT I
110 ' calculate and print check sum
120 IF (SUM < 10) GOTO 130 ELSE SUM = SUM - 10 :
     GOTO 120
130 IF NOT (SUM = 0) THEN SUM = 10 - SUM
140 Z$ = CHR$(SUM + ASC("0")) : GOSUB 190
150 ' print last long bar
160 GOSUB 370
170 LPRINT : LPRINT
180 END
190 IF (Z$ = "0") THEN GOSUB 570
200 IF (Z$ = "-") THEN RETURN       ' Ignore dashes (-)
210 DIGIT = ASC(Z$) - ASC("0") : SUM = SUM + DIGIT
220 ' Case Statement for each digit 1-9
230 ON DIGIT GOSUB
     390,410,430,450,470,490,510,530,550
240 RETURN
250 ' Initialize the printer for the correct number of
     bytes
260 OPEN "lpt1:" AS #1
270 N = 6*(K1-K2)                ' Set width of a digit in
     dots
280 RETURN
290 ' Print a long Bar then a space
300 FOR J = 1 TO K2 : PRINT #1, CHR$(255); : NEXT J
310 FOR J = 1 TO K2 : PRINT #1, CHR$(0); : NEXT J :
     RETURN
320 ' Print a Short Bar then a space
330 FOR J = 1 TO K1 : PRINT #1, CHR$(7); : NEXT J
340 FOR J = 1 TO K2 : PRINT #1, CHR$(0); : NEXT J :
     RETURN
350 ' TELL PRINTER TO RECEIVE ENOUGHT BYTES
     FOR A DIGIT
360 PRINT #1, CHR$(27)+"Z"+CHR$(N)+CHR$(0);:
     RETURN
370 ' PRINT A LONG ALONE
380 PRINT #1, CHR$(27)+"Z"+CHR$(K1+K2)+CHR$(0); :
     GOSUB 290 : RETURN
390 ' PRINT A 1
400 GOSUB 350:GOSUB 320:GOSUB 320: GOSUB 320
     : GOSUB 290 : GOSUB 290 : RETURN
410 ' PRINT A 2
420 GOSUB 350:GOSUB 320 : GOSUB 320 : GOSUB
     290 : GOSUB 320 : GOSUB 290 : RETURN
430 ' PRINT A 3
440 GOSUB 350:GOSUB 320 : GOSUB 320 : GOSUB
     290 : GOSUB 290 : GOSUB 320 : RETURN
450 ' PRINT A 4
460 GOSUB 350:GOSUB 320 : GOSUB 290 : GOSUB
     320 : GOSUB 320 : GOSUB 290 : RETURN
470 ' PRINT A 5
480 GOSUB 350:GUSUB 320 : GOSUB 290 : GOSUB
     320 : GOSUB 290 : GOSUB 320 : RETURN
490 ' PRINT A 6
500 GOSUB 350:GOSUB 320 : GOSUB 290 : GOSUB
     290 : GOSUB 320 : GOSUB 320 : RETURN
510 ' PRINT A 7
520 GOSUB 350:GOSUB 290 : GOSUB 320 : GOSUB
     320 : GOSUB 320 : GOSUB 290 : RETURN
530 ' PRINT A 8
540 GOSUB 350:GOSUB 290 : GOSUB 320 : GOSUB
     320 : GOSUB 290 : GOSUB 320 : RETURN
550 ' PRINT A 9
560 GOSUB 350:GOSUB 290 : GOSUB 320 : GOSUB
     290 : GOSUB 320 : GOSUB 320 : RETURN
570 ' PRINT A 0
580 GOSUB 350:GOSUB 290 : GOSUB 290 : GOSUB
     320 : GOSUB 320 : GOSUB 320 : RETURN
```

C VERSION

```
    /* zipbar.c for surf-mail */
    /* by Marshall Plann        */
    /* compiled fine in TC++   */
    /* 12/91                    */

    #include <stdio.h>
    #include <string.h>
    #include <fcntl.h>
    #include <ctype.h>

    #define PRINTER_PORT    "lpt1"
    #define ESC            27
    #define LONG            255
    #define SHORT           7
    #define SPACE          0
    #define K1            7      /* width of a space
*/
    #define K2            4      /* width of a bar
*/

    void write_bars();
    void bar_code();
    int  code_digit();

    unsigned char digit_bits[] =
{24,3,5,6,9,10,12,17,18,20};

    main(argc,argv)
    int argc;
    char *argv[];
    {
        int printer;       /* file to write to */
        char string[256];

        /* first parameter is the zip code or
else exit */
        if (argc < 2) {
            printf("Usage: %s
zipcode\n",argv[0]);
            exit(-1);
        }

        /* open the printer port */
        if ((printer = open(PRINTER_PORT,
O_WRONLY)) == -1) {
            printf("Error opening
%s\n",PRINTER_PORT);
            exit(1);
        }
        strcpy(string,argv[1]);

        bar_code(printer,string);    /* print the
bar code */
        write(printer,"\n",1);        /* print a new
line   */

        close(printer);
        return 0;
    }

    void
    bar_code(printer,str)
    int printer;
    char str[];
    {
        char out_str[255];
        int i;
        int digit;
        int count=0;
        int sum = 0;
        int len = strlen(str);
        /* add leading bar */
        count += code_end(&(out_str[count]));
        /* go through the string and
          create codes for digits */
        for(i=0; i < len; i++){
          if (isdigit(str[i])) { /* character is a
digit */
            digit = str[i]-'0';
            sum += digit;        /* accumulate for
checksum */
            if (count > 126) { /* dump every
128 bytes or so
                                to the printer */
              out_str[count++]='\0';
              write_bars(printer,out_str,count);
              count = 0;
              } /* end if */
                          /* code the next digit */
            count +=
code_digit(digit,&(out_str[count]));
            } /* end if */
        } /* end for */

        /* generate the checksum */
        if (sum > 0){
            count += code_digit( ( 10 - (sum %
10) ) % 10,
                        &(out_str[count]));
            }
        /* add trailing bar */
        count += code_end(&(out_str[count]));
        out_str[count++]='\0';
        write_bars(printer,out_str,count);
    }

    void
    write_bars(printer,str,count)
    int  printer;
    char str[];
    int  count;
    {
        char out_str[54];
        int num = 0;
        out_str[num++] = ESC;
        out_str[num++] = 'Z';
        out_str[num++] = count;
        out_str[num++] = 0;
        out_str[num] = '\0';
        write(printer,out_str,num); /* prepare
printer for data */
        write(printer,str,count);   /* write data
to printer    */
    }


    int
    code_digit(digit,str)
    int digit;
    char str[];
    {
        int i, j, k;
        for(i = 4, k = 0; i >= 0; i--){
            /*
            use digit_bits as a template
            for the bar codes.
            If a bit is on then add a long bar,
            add a short bar otherwise.
            */
            if ((digit_bits[digit] >> i) & 1){
                for (j=0; j<K2;str[k++] =
LONG,j++);
            } else {
                for (j=0; j<K2;str[k++] =
SHORT,j++);
                }
            for (j=0; j<K1;str[k++] =
SPACE,j++);
        }
        return k;       /* number of bytes added
*/
    }
    /* adds beginning or trailing bar */
    int
    code_end(str)
    char str[];
    {
        int j, k = 0;
        for (j=0; j<K2;str[k++] = LONG, j++);
        for (j=0; j<K1;str[k++] = SPACE, j++);
        return k;     /* number of bytes added */
    }
```

The Letter Bag

Governmental Nonsense

Dear 2600:

I've enclosed a piece of one of these junkmail things that my congressman sends out (at the taxpayers' expense of course). It's entitled "Pentagon Provides Job Information Hotline" and says the following: "The Defense Department has developed a telephone hotline to help employees who might lose jobs due to budget cuts and base closures. Those seeking employment are able to put resumes into a computer data bank that prospective employers can telephone to find workers with specific skills and experience. Applicants may call 1-900-990-9200 to register. There is a charge of approximately 40 cents per call. Interested employers can also use this number to obtain basic information about prospective workers."

It looks like the Defense Department is really bending over backward to help their laid off workers. They not only charge them 40 cents to get their resumes online, they also make sure that the service will be totally worthless by charging employers to look at the resumes.

Is this the Pentagon equivalent of a bake sale? Do they need another stealth bomber? What's next, reverse severance pay, where they dock your last paycheck for the privilege of being laid off? Now we see why the civil service is full of lazy idiots. Nobody that has any sense will work for them.

AB
Sacramento, CA

Various Bits of Info

Dear 2600:

I came across a little information liberated from a Pac Bell office in San Mateo, California. All information contained herefourth is in the 415 NPA.

Frame numbers (inside the switch) all seem to end with 0008. Some numbers for language assistance are: 811-6888 (Chinese), 408-294-0525 (Japanese), 408-248-5227 (Korean), 811-7730 (Spanish), and 408-971-8865 (Vietnamese).

Interesting numbers that also work in 415 are Coin Test at 0-959-1230 (useful for testing red boxes, only callable from payphones) and 811-1212 which responds to DTMF tones.

Ringbacks: 260, 290, 330, 360, 530, 550, 580, 740, 850, 870, 880, 890. Dial one of these plus the last four digits of your phone number. At the second dialtone, flash. At the steady tone, hang up. For free directory assistance (707, 408, 510, 415) dial 0+AC+555-1212 (within local BOC).

I'm going to buy a new computer to run a BBS. Primarily for file transfers, text files, and messaging. Any suggestions on what kind of system? 386/486, Mac, Amiga? I'm outta touch. Coppers took my equipment a few years ago in a raid.

The Crankster Gangster
and Tweaky Bird

For what you want, a Mac or Amiga would be too distracting. In other words, they're overqualified for simply running a board or doing transfers. For that, you're best off going with something along the lines of a 386 or lower, but how powerful you get is up to you. You can probably find a decent used machine for your applications at a fraction of the cost of a new one.

Dear 2600:

Hello there! I just wanted to tell you that I think your magazine is wonderful, and that I am going to have to subscribe to it now that our local bookstore has stopped getting it. Do you accept credit card orders? Or would you prefer a check?

By the way, I know that you collect info like this, so ANAC for (513) is 2002002002. This usually works but it seems to depend on what city you are calling from.

MG

Thanks for the info. But we don't take credit cards.

Hacking School

Dear 2600:

I have just recently received my first issue of 2600 and enjoyed it greatly, especially the USPS Hacking section.

I am an amateur and have a few questions to ask.

I go to a private college on Long Island and was wondering if there is any possible way to hack into the computer systems in order to change data that they have recorded, i.e., grades, records, classes, credits, etc. I believe all of the major computer systems are connected throughout the school via modem but no outside calls can be made. All I require is the password to get into the computer. Recently I went into the advisor's office and saw him type all the required stuff to get to my grades, all of which except the password. Do you recommend any suggestions on how to obtain the password? Is there any way I can connect via modem to hack out the pw or will it have to be done directly in the office?

Also in your Autumn 1991 edition, I read about receiving Caller ID Decoders for free through the 800 number. You also said that you would have to give your company name and application requirements. If you make up most of this information, will they check to see if it is legit before sending the ID's? By the way, what exactly do you mean by the application requirements, and do you have to know a lot about electronics in order to "put together" the Caller ID they'll send and will they send an LED or LCD display along or will I have to purchase that?

Could you print any locations for the Simplex locks on those Federal Express storage boxes?

Thanks for your help

MOE

There are more imaginative ways of getting passwords. Most of them involve people hacking, such as finding that special secretary who is dumb enough to practically walk a total stranger on the phone through the entire procedure. It happens all the time. Another possibility is to plant a bug of some sort and hope that at some point somebody casually mentions the password. Probably the best method is to convince them that you are calling from some kind of central organization and that they have to change their password immediately, either for testing or security purposes. As to whether or not you can connect by modem, one good way to tell is to see if they have a modem in the office. If so, does it appear to be hooked into several phone lines? If so, use the various tricks we've described over the years to get the number. By the way, if you're planning on changing grades and the like, we should tell you that the vast majority of attempts end in failure, sometimes colossal ones.

We have no idea how extensive a check the Caller ID decoder company ever performs. Why don't you try and see?

You can get a location of the nearest Federal Express dropbox (with fantastically easy-to-open Simplex locks protecting them: see Autumn 1991 issue) by calling 800-238-5355 and giving them a zip code.

Modem Voyage

Dear 2600:

I have been following your magazine for a while and find it very interesting even though my computer work mainly involves graphics and not telecommunications. I thought Emmanuel Goldstein's participation in the *Harpers Magazine* discussion was thoughtful and presented a more realistic face to the standard computer user stereotype.

I travel frequently in Asia and am curious about using a modem with my portable computer in countries such as China and Australia. What is involved in connecting to these phone systems? Will I need to purchase adapters or hardwire the modem directly to the line? I am completely unaware of where I can find this information. I contacted Southern Bell and AT&T and received the typical reactions: "You cannot do that... and why would you want to do that?"

CH

The best thing to do is to obtain the phone plugs when you get there. It won't be hard to wire them up. You should have no trouble using a 2400 baud modem unless you encounter C5 signalling, which is used on most long distance calls out of China, and some from Australia. In this case, you'll probably have to establish a voice connection first. Then (on the modem), the person you called would type ATA and you would type ATD to establish a connection.

Questions

Dear 2600:

I've learned through the grapevine that there is a computer program that automatically dials via a modem in search of carrier tones of computers that can be accessed. Apparently the program, without repetition, dials telephone numbers within a designated area code, and/or with a designated prefix, and stores those telephone numbers which provided access to computer carrier tones. Do you guys know of anything like this? I would really like to get my hands on a program like that. It would save many fruitless, red-eyed hours at the screen.

LH
San Diego

Your grapevine must be rather old. But that's okay - old as the information may be, it is still valid. Wargames dialers have been around since modems were first used. Some of the programs are in Basic, some in assembler, others in C. It's different for every machine. What you have to do is find someone with a program that will work on your machine. Ask on bulletin boards or check out our classified section on page 41. By the way, it's still open to debate as to whether or not scanning is illegal. Some phone companies will take action against scanners. We feel there's no harm in scanning, since you are not harassing any one person over and over but merely going one by one through a series of numbers in much the same way the phone companies do when they want to sell one of their overpriced services.

Dear 2600:

I want to know where I can get the following items: 1) The best "Wargames" autodialer that you know of. 2) Back issues of *Phrack* or any other similar periodical.

I don't consider myself a hacker or anything. I just want to start reading about it and start learning all I can. I just hope that you are not the type of people that couldn't give a shit about anyone who doesn't know anything about it.

I used to run a BBS about four years ago. It was pretty big, until I got shut down by someone who had friends at the phone company who didn't like me or the people who were calling my board.

I don't know what I could offer you right now. All I have access to are credit card numbers, but it doesn't sound like you are into that kind of thing.

John

Yeah, you're right about that one. Credit card numbers are incredibly easy to get. If only they were useful for something other than stealing...

See the previous letter for our speech on Wargames. As for Phrack, try anonymous ftp at ftp.eff.org or ftp.cs.widener.edu. It can also be found on bulletin boards like Salsbury Hill which can be reached at (301) 428-3268. You can subscribe to Phrack if you have a network address by following these instructions: Send mail to listserv@stormking.com leaving the subject field blank. The first line of your mail message should read SUBSCRIBE PHRACK (your name). Don't leave your address on this line. You'll get a confirmation message. You should then receive Phrack from phrack@stormking.com. If you have problems, contact server@stormking.com with *for details.*

Dear 2600:

Are you interested in knowing the internal numbers of Southwestern Bell such as verbal ref or numbers?

Also, ANAC numbers: South Padre Island, Texas: 943; Port Isabel, Texas: 970

John

Why of course we're interested! What a silly question.

Dear 2600:

I love your magazine. I've built the modified tone dialer (over eight of them), and it works great. I'm currently building a mag card copier. There's a store called Weird Stuff Warehouse in Mountain View, CA which was selling card readers for 10 bucks! So I picked up a couple. I'd like to know a couple of things though. First, when I use the coin dropper dialer, the operator voice keeps coming on every five minutes to ask me to insert more money. This is really annoying especially when I want to use my portable computer to communicate over the phone! I've heard there's a tone that you can put on the line that allows you to get some kind of operator privileges. There was a letter in your Summer 91 mag from a guy using the tone from home in Canada who was caught. Could you please explain exactly what the procedure is for getting access to this? I can generate whatever tones are needed. I just don't know the procedure for doing it. I'd really appreciate it if you could fax the info to me, or if you have some stuff for me to buy, I'll send you money. Is it possible to fax checks?

Also, I recently bought a cellular telephone from Radio Shack. They had a special sale on one for $199.95! I've taken it apart. It uses a standard processor and I've dumped the Eprom's, but have yet to find a disassembler for the processor. Do you have any info on how to hack these things?

As I said I'm currently assembling a mag card copier. I'm going to use it to copy BART cards. These are mass transit cards for the train system in San Francisco. I'll let you know how well it works.

E

Bay Area

Forget about faxing checks. Unless you're able to find a way of blue boxing in California and assuming you don't want to use other people's calling card codes, you're pretty much stuck with the obnoxious lady asking for money or, in your case, little beeps. But you can deposit an awful lot of money in advance for calls within Pacific Bell, up to $100. AT&T is much more restrictive, only allowing you to go 35 to 45 cents above what they demand. (We've published all kinds of blue boxing articles in the past if you think you've found a way to make use of them.)

The call is out for cellular phone dissection info.

Be careful copying BART cards. We're told the mag card copier we featured was actually used to do just that.

Dear 2600:

I feel your publication serves a valuable purpose in today's technology-oriented society. Two questions, however. Isn't what you're doing somehow illegal? If so, have the cops pressured you for information about hacking/phreaking activities?

RA

Virginia

(I'm not a cop!)

Congratulations. In answer to your first question, we publish a magazine about hacking. As long as the First Amendment exists, we're completely within the law. A magazine called TAL in California was shut down by the phone company in the seventies for printing similar information. We believe this action was illegal and in direct contradiction of freedom of the press. Since nobody has challenged it, their action stands as if it were legal. Fortunately we haven't yet gone down that road in New York. In answer to your second question, no.

Abuse of SSN's

Dear 2600:

Our school uses Social Security Numbers as student identification (Tacoma Community College). I've heard that this is not a good idea and have tried to convince the Administration that random numbers should be used but they said since they're not expressly prohibited from using SSN's, there's no reason to change.

What are some of the damaging things that a person can do when he has someone else's SSN? Is there more info needed? At the least, what are some annoying things that can be done? If I had some specifics, I might change their minds.

RH

Tacoma, WA

Once you have someone's Social Security Number, you can do almost anything to them. That is hardly an exaggeration. In fact, to prove a point, why don't you ask your administrators to give you their SSN's. If they're so concerned there's no harm. Once you've got their number, you can convince almost anybody in authority (banks, credit agencies, schools, the government) that you are in fact them. Plus you can get all kinds of information about them using this number as verification. This leads to even more information and a great deal of power. We suggest you read the article in our last issue (Autumn 1991) entitled "Protecting Your SSN." Also, read the next letter for another perspective. By the way, 2600 welcomes contributions of high-ranking government SSN's. What's good for the goose...

Private Eye View

Dear 2600:

I want to commend you on an excellent publication that is needed. Keep up the good work! If I

may, I'd like to comment on your role in our society and also on your article "Psychology in the Hacker World."

Although I am not technically a hacker I used to be in a similar field of endeavor. Presently I own a small company that has produced an artificial intelligence software used to handicap horseraces. It can learn what the profile of the winning horse is in a series of races and then predict how today's race will do.

For the previous five years I was a private investigator and before that I was involved in law enforcement.

From my time working with law enforcement people and then in the private investigation field I came to understand the effects that power and authority can have on people. It can be subtle and devastating. Much like your article on "Enforcers", law enforcement people can take on a religious zeal about them when dealing with laws, people, and their jobs. It seems that we forget something basic about laws. There are two types of laws for crimes that have existed for civilized man. In Latin they are called Mala In Se and Mala Prohibita crimes. Mala In Se crimes are those that any person would naturally say is wrong. Murder, rape, etc. In other words, Mala In Se crimes would be acknowledged by most humans any time throughout history.

Meanwhile, Mala Prohibita crimes are those that are wrong simply because we say they are. Parking in a red zone, hacking a computer system, writing bad checks, smoking marijuana, not paying your restaurant bills, etc. These crimes would not be considered wrong by the majority of humans that have lived throughout the history of mankind. What is interesting to me is that the "enforcers" (i.e., law enforcement people, religious people, politicians) have such a zeal in regard to Mala Prohibita crimes, and then only selectively.

Along this line I also wanted to mention a thought for you to consider. It seems that our "leaders" are at an all time low as far as personal morality and responsibility, both to their own people and to the country at large. In government we have bounced checks to the tune of $10,000 (on accounts that had been closed for a year), not paying bills, excessive waste ($180 million/year according to GAO), and spending on things that are amazing. During the Vietnam War we had Conscientious Objectors who, for various ethical, religious, or moral reasoning, could not fight in or support the war. It seems to me that we as Americans should literally be very ashamed of ourselves for supporting and allowing the governmental farce to continue. I've wondered why there has not been an uprising; perhaps it is because of the sheer size of the country and the number of people (politicians, bureaucrats, government workers, contractors, accountants, lobbyists, aides, lawyers, etc.) who are dependent on the system remaining the same. I have an idea - why don't we start a campaign (t-shirts, bumper stickers, etc.) called C.O.G. - Conscientious Objectors in Government.

One final thought in regard to hacking. As a private investigator, I spied on people in various ways. I found people who didn't want to be found and learned things about people who probably didn't want it to be known. I've enclosed a list of database companies that P.I.'s can access to gain info on you. It's always been said that if I have your full name and your date of birth or Social Security Number, I own you. There are ways in fact to affect a person's life by the way you gather information on them! The list deals with companies that sell public information which is quite legal. I have another list of people I could call and get anything else on someone I wanted (as long as I can pay for it). There is no security. If you have the money, you have the information.

Not too long ago you could get California DMV information for about $5.00 per name or vehicle license number. A weirdo killed a TV sitcom star on her doorstep after gaining such information from a P.I. in Arizona. Immediately the government stepped in and made DMV info classified so that P.I.'s (and the general public) could not get it. Did it work? Are you kidding, we didn't need it directly from DMV anyway. All the law did was decrease legitimate income for some of these database owners (quite a bit of income, by the way) and created an underground market. Information is big business, bigger than most know.

I'm out of the P.I. business. It is stressful and not all that glamorous, and there are ethical concerns about invading people's privacy. But I can understand the basis of hacking, i.e., curiosity... it applies to that field also.

Keep up the good work, someone has to be the watchdog in the computer area.

PW

The list of database companies appears on page 46.

Call For Info

Dear 2600:

Together with a friend, I am writing the Cyberpunk Manifesto and will be publishing it in a volume titled "The Cyberpunk Manifesto and Related Articles: The Achievements and Goals of the Freedom of Information Movement, a Guide for Hackers, Phreaks, and Other Techno Subversives." We are currently searching for submissions of articles by others involved in the F.I.M. to include under the related articles section, as well as what you think the manifesto should say, so that our ideas are not necessarily the only ones represented. Articles on computer security, networking and telecommunications, the Information Age, information in general, hacking, phreaking, copyright, viruses, politics, music, art, philosophy, and anything else are what we are looking for. Technical articles are good but include why as well as how. If we make enough money, or can find outside financing, we may start a new cyberpunk publication which we would want to have articles by hackers, not just technojournalists.

If interested, write to Christian X., The Invisible Hand (T), Simon's Rock College, Great Barrington, MA 01230.

On Virus Books

Dear 2600:

The book that CH inquired about in the Summer '91 issue is titled *Computer Viruses and Data Protection*, and the author is Ralf Burger. It is available from our good friends Loompanics Unlimited, PO Box 1197, Port Townsend, WA 98368. I won't say it's not worth the bucks ($18.95), but Burger does have some weird ideas about the concept of providing value for money: he is cutesy-coy about withholding source code that the buyers of his book - unlike the great man himself - are presumably too stupid to be entrusted with. He will *maybe* condescend to provide the withheld information if you send him extra money and agree in writing to go to jail if you modify the code, show it to anyone else, or *attempt to run it*.

No joke, folks - you pay your money and you get a program you are *forbidden to execute!* While we're critiquing you, Ralf, for nineteen bucks a pop you might want to get somebody familiar with English spelling, grammar, and syntax to proofread your translation from the German.

Much better value for the money is Mark Ludwig's *Little Black Book of Computer Viruses* ($15 from American Eagle Publications, Box 41401, Tucson, AZ 85717). Ludwig is responsible enough to warn of the dangers of his subject, but, this accomplished, then proceeds to provide *all* the information his readers could wish: historical background, detailed exposition, and well-commented source code.

Keep on hackin'
Phat Pharddy Phreak

Long Distance Trouble

Dear 2600:

At about 01:00, Saturday, 11/17/91 I noticed some trouble with the MCI network. I tried calling MCI MAIL using their 800 number and calling from upper Manhattan. I got a New York Telephone intercept recording that "all circuits are busy now." I tried a few other times and got the same message. I then called 10222-1-700-555-4141 to check it out and got the same intercept. I then tried 10222-1-617-nnx-yyyy and got the same response. I was able to get through to the real number in 617 land with the other carriers. But the problem this illustrates is: how do you get around a blocked or defective 800 switch when you don't have an alternative "real" number for the location?

Danny
New York

You don't. Unless you can contact the long distance company that operates the 800 number and ask them for a translation. But it would probably be hard to reach them anyway if their entire network was down. One more example of technology moving backwards.

Dutch COCOT's

Dear 2600:

In Holland quite a few companies and institutions own coinvoxes (comparable to COCOTs). Normally you're not supposed to be able to call Telecom payphones (regular ones). With coinboxes it's simple. Just call the company and say you're a Telecom employee and tell the technical staff (if any, otherwise the operator, etc.) that you have to check the lines because there's a break in the cable and you need to have the coinvox's phone number to be able to see whether it's this line that's causing the problem.

Once that's done, take your DTMF dialer and go to the phone and have the phone forward your call by pressing *21* (your phone number) #. To use it call 06-0410, tell them to call you back (at the coinvox's number) because "you can't bill it direct because of administrative problems." They'll call you back and bill it to the coinvox's number. If you don't need to call from home, you can of course do it directly.

Note: make sure to change to another coinvox regularly (once a month) and to erase your number from the coinvox!

Jack-❖
Hengelo, Holland

Cellular Eavesdropping

Dear 2600:

I recently picked up a copy of your publication and enjoyed it alot. I have a question with regards to the 800 Mhz band. Is it possible to use an old VCR or TV with channels 73-83 NTSC standard (824-890 Mhz) to receive cellular telephone conversations for experimental purposes only? What is the address of the subscription department of *TAP*?

Matt B.
Somerset, MA

It most certainly is possible and it's done all the time. But you need a set with a UHF dial that doesn't click so you can fine tune more easily.

The last address we had for the new TAP was PO Box 20264, Louisville, KY 40250. But we haven't heard anything from them in quite some time. The old TAP stopped publishing in 1983.

COCOT Experimentation

Dear 2600:

After reading the list of COCOT numbers in your previous issue (Autumn 1991), I decided to experiment a little more with the phones. After the "thank you" by the operator, four tones are played. I used my tone decoder and found out that there were a few different sets of tones played. The most commonly encountered set was "AB87" and two others were "AB45" and "AB23". I have not found any COCOTs which did not play one of the above three sets of tones. I have messed around with them for a while, but I haven't come to any conclusions. If anybody knows about these tones, please write in and let us know.

Kingpin @ LoST - RL

Credit Wanted

Dear 2600:

In your Autumn 1991 issue on page 40 you have an article entitled "More Conversion Tricks" by DC. At the beginning of the file, DC writes: "I have come across a file explaining how to make the conversion but incorporating a switch to select between the two different frequency crystals, enabling both touch tones and a red box. One thing I didn't like about the file's design is that it had wires coming out of the back of the unit to the two crystals and the switch which were all epoxied together to the back of the unit. Ugly. I managed to fit everything neatly inside the unit."

Obviously, DC has read the file I released into the net. I take offense at his remarks and attitude. First, he *bases* his article on my file's idea for the toggle switch conversion, yet he gives me *no credit*...he could have at least mentioned my name. He offers an "improvement" by putting the crystals and the switch inside the box. Then he criticizes my file's design! In my file, I explain that my design is a *quick hack job*. I wrote that file to enable even the poorly coordinated to slap together the toggle switch conversion without any difficult filing or soldering. To me, it was more important to get the toggle switch conversion into as many people's hands as possible. I didn't want a tricky, slick-looking box...I wanted something *anyone* (even people with all thumbs) could build and use.

I'm not really *pissed* at DC. Maybe he just forgot my name or whatever. I just feel a bit slighted, and I believe in giving people credit where credit is due.

Count Zero

POSTNET Correction

Dear 2600:

Some rectifications and extra information regarding the USPS Hacking article (page 32 of Volume 8, Number 3).

The POSTNET on page 32 does not encode 2600's ZIP+4: 11953-0752. It consists of a combination of 21 long bars and 31 short bars (and not the usual 22 long bars and 30 short bars as stated in the third paragraph). In order for the POSTNET to encode 11953-0752, one must apply the following modifications: add short bar, position 2/52; delete short bar, position 47/52; change to long bar, position 38/52; change to short bar, position 42/52; change to long bar, position 46/52.

It is obvious that the error was due to misprint, but some of the readers might not have understood the first part of the article because of it. Have you decided to mail the sample letter printed on page 35? If so, have you received it yet?

The number, length, width, and space separating horizontal bars for business reply mail on page 35 also seem to be relatively arbitrary.

Black Fox
NYC

We did in fact make a mistake with that POSTNET. Quite a few readers caught it. Corrections and addendums appear on page 31.

On Prodigy

Dear 2600:

I don't usually write to you with my real name and address but what the hell. I have nothing to hide. I think your latest (Autumn) issue is your best ever! Bravo! It is full of very interesting and juicy information. More importantly though, it defines the hacker spirit and ethic that has been smacked and feared by ignorant people. I've bought a number of issues to give away to friends and associates who ask me what hacking is all about and who think I'm part of some devious underground. Your magazine, along with the books *Hackers* and *Cyberpunk* are necessary reading for people wanting to learn what hacking is all about.

Now unto other things. Big Al has a letter in your latest issue about Prodigy reading private information from his machines to their own. He mentions the STAGE.DAT file as the hiding place. I have checked my own STAGE.DAT and found nothing really suspicious except for a list of subdirectory names from one of my hard drives. The list is somewhat selective and includes more Compuserve subdirectory names than anything else. Unless other data is somehow scrambled into this file, I can't find evidence of what Big Al is talking about. I'd be curious to hear more about how he found his data (encrypted, hex, ASCII, etc.) within the STAGE.DAT file. If what he has suggested is true, then it should be made widely known. It seems to me that Prodigy may even be violating the law by stealing private information. Sure, the super of my building has the keys to my apartment, but if I ever found him rummaging through my closets, I'd call the police. That is, after beating the crap out of him!

After giving all of this some thought, I think we should be very careful about trusting online services with our computers. It is obviously very easy for them to read our files, copy information, and use that information without us ever knowing it. I'm used to Prodigy and Compuserve spinning my hard drive when I'm online. I never stopped to think about what they might be doing until now...

Lawrence
New York

Dear 2600:

Unfortunately, in his letter on Prodigy in the Autumn 1991 issue, Big Al proves nothing other than his ignorance of how MS-DOS allocates disk space to files. That disk space was once used for a file in subdirectory A, which was deleted and has no bearing whatsoever on whether that disk space can later be used for a file in subdirectory B. It would be proof of strange behavior only if data was migrating across disks, either logical or physical.

I don't know enough about Wordstar to know how it manages temporary files, but assuming that it behaves normally for a word processor, the most likely scenario for Big Al's test goes something like: a) While creating a dummy document with a dummy name in it, Wordstar creates a temporary file, which ends up containing most or all of the document being worked on. b) Wordstar is halted, and while cleaning up it deletes the temporary file. c) Prodigy is started and when it asks MS-DOS for disk space for STAGE.DAT, it gets that disk area that was most recently freed up (this step can vary depending on MS-DOS version and whether the hard disk has had all of its area used since it was last formatted), which naturally contains all the junk from the Wordstar session. I consider this a much more plausible scenario than Big Al's assertion that this proves that Prodigy is reading data out of Wordstar document files.

If Big Al wants to prove anything here, he should use Norton Utilities or the equivalent to overwrite all unused disk sectors and then see if Prodigy puts anything into STAGE.DAT. Or he should check the sectors that will be allocated for the next file opened both before and after Prodigy is started, to see what Prodigy changes.

As for the names of computers such as ABLE LEGAL and BAKER LEGAL showing up on a Prodigy mailing list, is he absolutely certain, cross-his-heart-and-hope-to-die, that no one registered some of the software associated with the network using the machine names?

So while I agree that the Prodigy affair may have been glossed over mighty quick, there are limits to paranoia on the topic before it gets really silly.

If you do want a scandal, start thinking about how many computer technicians don't realize that using Norton's WIPEFILE on your word processor file isn't enough unless you hunt down and wipe out all the temporary files your word processor used too.

Jon Radel Reston, VA

It's been our position that even if Prodigy was doing nothing wrong, unsuspecting users are opening up their personal systems to outside entities (not hackers) which could one day do quite horrible things. We hope this realization is enough to wake most people up.

Reading ANI

Dear 2600:

I have a Sprint 800 line. I called a Sprint representative to ask about Caller ID. She didn't know offhand but said she'd check with the proper technical people. She very helpfully got back to me the next day. She told me the Caller ID is generally available to their large volume users but the digital pulses are sent out to the private 800 users too. Next I bought a Sears Caller ID unit - an AT&T model for $59.95 with a 14 number memory - an excellent price compared to what's been offered by some mail order places in the back of electronic/hobbyist magazines. I had two friends in different parts of the country call on the 800 line but the LCD screen on the Caller ID unit remained blank. Apparently the local telco either doesn't/can't transmit the information between rings or they simply filter them out even on the 800 line. My 800 number is piggybacked onto my home phone so it's actually redialed from Sprint somewhere out in the cornfields of Nebraska or Kansas.

Your postal hacking article was very informative. You can mail standard size letters of less than one ounce with any postage denomination value - even cancelled stamps - and they'll almost always go through. Just make sure they are addressed neatly with the zip code written out clearly in nice block digits and mail them singly in a busy mailbox - like a drive-up one or the kind at a shopping mall that gets a lot of volume. Probably the best way is to use 4 cent stamps and if there were any questions you could say the old 25 center must have fallen off. I pay my bills with this method and even send personal letters to friends and none of them has had to pay postage due.

Your magnetic stripe card duplicator article was most interesting. I'm still in the process of getting the parts together (for tape heads try All Electronics, PO Box 567, Van Nuys, CA 91408 - their catalog has used/surplus card reader assemblies). Here at Akron U. the photocopy machines use a card with a thin audiocassette-width magnetic stripe on it. The cards are sold from a vending machine in $1 increments with a $20 maximum value. It looks to be just a single track of information on it and should be easy to clone using the read/write circuit in the article. If successful I'll let you know and send along a photo of my completed unit.

Pete at AU

What is transmitted to 800 numbers is not Caller ID, but ANI. There is no way a Caller ID box would work on the terminating end of an 800 number for what you want to do. The ANI data is coming from the long distance company that operates the 800 number. They in turn get it from the caller's local company. The local company on the receiving end is not interactively involved in passing this data, unlike Caller ID. It sounds as if your local company isn't using Caller ID at all or you would have gotten an "Out of Area" or equivalent message when your phone rang rather than a blank screen.

By the way, your letter was mailed with a 29 cent stamp. We hope that was intentional.

Red Box Warning

Dear 2600:

A lot of you have probably modified the Tandy (Radio Shack) dialer and found it to work as a red box. I used a similar, but safer mod a number of years ago when I lived in the USA. I would like to point out a grave danger in actually using this modified device.

(continued on page 40)

Class Features

by Colonel Walter E. Kurtz
75 Clicks from the bridge

Centel in Las Vegas has Caller ID, along with several other features recently added to its custom calling features. The local system has a privacy feature which can be permanently added to a phone line by the phone company (and it can't be deactivated without calling the phone company, which may be a problem if you try to call someone with Caller ID Block Rejection activated), or on a one call basis by dialing *67. The permanent add-on is only available for residential lines, and every customer gets the one time feature. The following features (and codes) are what is currently on my phone (although some of them are only available in two central offices and for residential only at present).

***57 Call Trace:** This is a special number to call to trace problem calls. It will trace the last call. There is a charge for the call and the number is only given to the police.

***60 Call Screening:** This will reject up to twelve numbers. Up to twelve numbers are stored and the feature can be activated or deactivated at any time without reentering the numbers. You can add or delete numbers. Only local numbers can be entered. You can store the last number dialed even if it has Caller ID Block. No long distance, cellular, or trunks (as used by hotels or larger PBX). The calling party hears a recorded "The number you have dialed is not accepting calls from you at this time," followed by a disconnect. Your phone doesn't ring. You can store the last number which called you, even if you don't know what it was. This includes Caller ID blocked calls.

***61 Distinctive Ringing:** This will cause your phone to ring with three short quick rings, instead of one long ring. The distinctive ring usually doesn't activate electronic key systems. The feature has a twelve number (local only) capacity. You can store the last number which called you, even if you don't know what it was. This includes Caller ID blocked calls.

***63 Preferred Call Forwarding:** This will call forward only up to twelve phone numbers (local only). The rest of the world will ring your phone as normal. The feature has a twelve number (local only) capacity. You can store the last number which called you, even if you don't know what it was. This includes Caller ID blocked calls.

***66 Auto Redial:** This will call the last number you called, whether it was busy, answered, or unanswered. It will continue to redial busy numbers for up to 30 minutes or until cancelled by calling *86. It works by checking the line every few seconds until it senses that it is free. Your phone will ring, and when you answer, the other party's phone will ring. It's not fast enough to call back to those annoying mass-dialing junk callers. This feature will work with any local call including Caller ID blocked calls, but not cellular or trunk lines.

***67 Caller ID Block (one call):** This will display a "Private Caller" message on Caller ID displays. Caller ID blocked calls can be stored in the Call Screening, Distinctive Ringing, Preferred Call Forwarding, and Selective Call Acceptance lists, but the numbers are not given out when the numbers are listed. Only the total number of private numbers is listed, and they must be deleted as a group.

***68 Selective Call Acceptance:** This is the opposite of Call Screening. Up to twelve local numbers can be stored and they will be the only calls which will ring your phone. All other numbers, including long distance, cellular, and trunk lines will be rejected with the same message as Call Screening. This can be used to avoid creditors and still talk to that special someone. Combine it with Caller ID or selective call forwarding to play hooky from work.

***69 Return Call:** This will give you the last local number called, and you can redial it by dialing 1. It will give you the last number even if you do not have a Caller ID box. (Great to use if you don't have a box by every phone.) If it was a Caller ID blocked call, a recorded voice will announce, "The last number that called your line cannot be given out. If you want to call this number enter 1, otherwise hang up now." If the last call was a cellular number or not a local call, the recorded voice will advise you, "We're sorry. The last number that called your line is not known. Please hang up now."

This can be used with Caller ID Block to call back the last person who called you if their call was blocked. Just dial *67, *69, 1.

***70 Cancel Call Waiting (one call):** This will deactivate call waiting for the duration of one call. A good way to send faxes or use a computer without getting dumped. Include it in Hayes compatible dialing strings as ATDT*70W5551212. The W will make the modem wait for the dial tone and is easier than a bunch of commas.

***72 Call Forwarding:** Makes all calls forward to another number. If used with Caller ID, the calling party's number will show up on the number which you've forwarded your calls to. Example: You forward your phone to 555-1234. 555-3825 calls you. The Caller ID box at 555-1234 will display 555-3825, not your number. Numbers can be forwarded to any 7 or 10 digit number. 411, 611, 911, 118 (time) won't work. If you forward to a long distance number, you will be billed for the calls.

***73 Cancel Call Forwarding:** Deactivates Call Forwarding.

***74 Speed Call (8 numbers):** Stores memory dial calls. You can call someone by dialing one digit. Calls faster if you follow the number with a # sign.

***75 Speed Call (30 numbers):** Similar to above but holds 30 numbers. These only work for phone numbers, and can't be used as numbers for back-by-phone, alternate long distance, or other services. You'll have to use a phone-based memory system. The problem with all memory phones is that it causes the brain to not remember phone numbers. Remember this next time you try calling someone with an unpublished phone number from a payphone by dialing 7#.

***80 Caller ID Block Rejection:** This feature is a lot of fun. If anyone has Caller ID Block activated, they hear a recorded message which advises them, "The party you dialed does not accept blocked calls. Please hang up and call back with your caller identification unblocked." If they have permanently added Caller ID Block to their line, they will have to call the phone company to have it removed, or call from another phone (neighbor's, payphone, cellular phone, etc.).

***81 Cancel Caller ID Block Rejection:** This accepts Caller ID blocked calls.

Most phone companies use the same numbers for regular (non Centrex) lines.

Another phone type is Centrex. This is only available for business lines, but you can get one line service. Probably the neatest feature is call transfer. If you call me, I can put you on hold (with a switch hook, just like 3-way calling), call another party, and then hang up. If I wait until they answer, you will hear the third party's voice. Otherwise you will hear the ringing signal. My phone is now free and you are connected directly to the third party as if you called them yourself. I can call anyone, local, long distance, or cellular. If the party I called has Caller ID, the display will show my number, not yours. There are other features like no-answer call-forward and busy call-forward, but some of the stuff listed above is not available.

If you want to avoid your number being displayed on Caller ID boxes, 800 ANI, 911, etc., use a cellular phone. If you use the call forwarding feature in your cellular phone, you can avoid airtime charges in some cellular systems. The Caller ID boxes display "Unknown Caller", same as for long distance calls. 800 ANI and 911 systems receive the phone number of the cellular switch, not your number. Example: If your cellular is 555-7606, the 800 ANI display shows 555-1050. The cellular company computer tracks all calls placed on your phone, so don't try this with anything of a sensitive nature. Remember, cellular phones are radios, so even though it's illegal to monitor conversations (another brilliant piece of legislation from Congress), Bell Atlantic Cellular in Washington DC offers scrambling from the car to the cellular switch.

COCOT CORNER

Welcome to the amazing and unpredictable world of COCOT's, those strange payphones that don't quite work the way regular payphones do. On these pages, we hope to show you what is unique and precious about these phones that everybody loves to hate.

Here are some orders taken from a COCOT company's database. It covers a two week period in a two state area. Each line represents orders the repairman must follow for a particular payphone.

CALL OWNER TO POWER UP PHONE
REMOVE PHONE - OUT OF BUSINESS
INSTALL ON PEDESTAL-NEW LINE
INSTALL NEW LINE-SM SHELF
RE-INSTALL PHONE AFTER THE FOURTH
REPLACE LOWER HOUSING - BLOWN UP
COLLECT $151.00 AFTER 4 P.M.
PLEASE INSTALL EXT RINGER ON PAY PHONE
REPLACE BOARD SEE STEVE
COLLECT $156.10
OPENING 7/17 - READY FOR PHONES
NUMBERS ARE STICKING
COLLECT $143.15
COLL $150.90
COLL $138.80
COLL $140.00
COLLECT $158.79
COLLECT $156.80
GLASS IS BROKEN IN ENCL
MOVE PHONE TO OPPOSITE WALL-NEEDS EXT
PHONE IS EATING MONEY
L/D TEMP. DISCONNECTED
PHONE NOT TAKING COIN
DROP WIRE IS HANGING/CONDUIT BROKEN
PHONE EATING $
COLLECT $129.80
COLLECT $127.58
COLLECT $126.30
COLLECT $126.35
COLLECT $140.85
COLLECT $129.65
COLLECT $136.46
COLLECT $156.45
COLLECT $157.66
COLLECT $127.68
REMOVE PHONE THURSDAY 10 A.M.
REMOVE PHONE - OUT OF BUSINESS
NO ANSWER EITHER PHONE
WAITING FOR DROP - DROP WILL BE 21ST
INSTALL NEW LINE PEDESTAL
INSTALL NEW LINE PEDESTAL
STILL ON COIN SUPERVISION
NEEDS NEW LOCK PER ARTIE
PHONE IS EATING MONEY
COIN JAM
COLLECT
COLLECT
COLLECT
COLLECT
HANDSET MISSING
INSTALL NEW LINE PEDESTAL
INSTALL SMALL SHELF NEW LINE
INSTALL NEW LINE BACKPLATE
INSTALL NEW LINE PEDESTAL
REMOVE PHONE & ENCLOSURE
NO DIAL TONE
PHONE NOT TAKING DIMES
NEEDS A NEW COIN RETURN LINKAGE
CAN'T CONNECT WITH INET
NO ANSWER WITH INET
NO ANSWER
INSTALL NEW LINE PEDESTAL
INSTALL UPSTAIRS ON BACKPLATE
CAN'T HEAR ON PHONE
PHONE IS EATING $
PHONE IS EATING MONEY
START THE WIRING PLEASE-STOCK COMING MON
START THE WIRING CONCENTRATE ON THIS ONE
CHECK OUT THE WIRING
CHECK WIRING

The following messages were generated when the company called out to various payphones to retrieve data from them.

GET BILLS SUCCESSFUL
GET BILLS SUCCESSFUL
NO ANSWER
GET ERROR WORD SUCCESSFUL
GET BILLS SUCCESSFUL
HARDWARE ERROR
HUMAN ANSWERED PHONE
SET TIME SUCCESSFUL
GET BILLS SUCCESSFUL
LOW ACTIVITY
HARDWARE ERROR
GET ERROR WORD SUCCESSFUL
NON-INTELLICALL INCOMING CALL
WARNING: INCORRECT DATE/TIME
COMMUNICATIONS ERROR
GET BILLS SUCCESSFUL
HUMAN ANSWERED PHONE
MAX RETRIES REACHED
LOW ACTIVITY
GET BILLS SUCCESSFUL

The following is part of a letter from a COCOT representative to a customer explaining how operator assisted calls work. While these payphones seem equipped to reach almost any long distance companies, the representative unwillingly admits involvement in a scam. When placing collect calls, the phone assumes a yes answer after five seconds. This is hard evidence that Integretel makes unauthorized collect calls as course of habit. Any phone that picks up with an answering machine will be billed if an Integretel collect call is coming in. Keep that in mind when you look at your next phone bill.

"Dear Mr. X,

"This letter is to explain how our payphones work with regards to 'store and forward' technology. We refer to this type of phone as an Intellistar payphone. The caller has many choices in placing collect and credit card calls. They are prompted, as we will show, how to place these calls and how these calls are billed.

"The caller may use 10XXX, 950-XXXX, and 800 access numbers, or operator assisted numbers to use the long distance carrier of their choice. In addition to these choices, we have programmed a speed dial *number. STAR (*3) THREE to reach AT&T. Also a caller is able to reach AT&T by dialing double zero (00) or 10288O. Other long distance carriers have similar 10XXX numbers for their card holders to access their networks, insuring freedom of choice on our payphones. All phones have labels instructing customers how to dial in a conventional manner.*

"The Primary Inter-exchange Carrier (PIC), is AT&T on all phones [at your site]. This allows the phone to use AT&T for all long distance coin calls.

"Now we would like to take you through each type of zero plus call that can be made on our phones. These calls are:

"1. Zero Minus (0-) ...zero dialed only

"2. Zero Plus Seven (0+XXX-XXXX) local and toll

"3. Zero Plus Ten (0+NPA-XXX-XXXX) interstate

"The following is the dialog heard:

"0-(Zero Minus) - Dialog #1:

" 'This is your operator. To place a collect call, dial one. For operator assistance, dial zero.'

"If nothing is dialed and the caller waits, or zero is dialed, phone will automatically dial International Telecharge, Inc. (ITI) and will speak to a live operator.

"When the caller dials one, the phone then prompts: 'Please enter the number you wish to dial now.' Then 'After the tone, please state your name.'

"The caller's name is recorded (stored) and then played back (forwarded) to the terminating number. The called party answers the call and hears, 'Hello, you have a collect call from (name). To accept this call press one, or hang on. To refuse, dial zero.' This message will repeat again. If the call is accepted by dialing one, the telephone will state 'Thank you for using Integretel.' In the case of collect calls, the called party is charged for the call. If the called party is equipped with a rotary type phone, the call will be accepted after five seconds. And if the call is refused by dialing zero, the call is terminated with a message that states, 'This is not a billable number.'

"0+7(Zero Plus Seven):

"When a call is placed by dialing zero and seven digits, local or toll, the customer will hear the familiar 'bong' followed by the name 'Integretel'. This is known as branding. This is to identify the billing company. The dialog is as follows.

"Dialog #2:

" 'This is your operator. Please enter your calling card now, or to place a collect call dial one. For operator assistance, please dial zero.'

"If the calling card number is entered, the phone will now say 'Thank you for using Integretel.' The call will be completed and charged to the card holder by Integretel. If the call is a collect call, the same events take place as the zero minus call. (See Dialog #1.) If operator assistance is requested, the local phone company version of store and forward is employed. At this time, the caller can speak to a local phone company operator.

"0+10(Zero Plus Ten):

"When this type of call is placed, the caller will hear the familiar bong followed by 'Integretel'. The dialog is as follows:

"Dialog #3:

" 'This is your operator. Please enter your calling card number or to place a collect call dial one. For operator assistance, please dial zero.' If the calling card number is entered after the first bong, the caller will hear 'Please wait one moment.' At this time, the calling card is being verified. After a few seconds the phone will again say 'Thank you for using Integretel' and the call will be placed. If the calling card is not verified the caller will be automatically routed to an AT&T operator.

"If the caller decides to use operator assistance by dialing zero, the phone will state 'Please wait one moment' as it speed dials ITI. The caller then hears a bong followed by 'ITI'. 'Please enter your calling card number or zero for an ITI operator now.' When the card number is entered the caller hears 'Thank you for using ITI' and the call is immediately placed. If zero is dialed, the ITI operator will answer.

"International Telecharge, Inc. is an Alternate Operator Service (A.O.S.) located in Dallas, Texas which has a reciprocal agreement with all Regional Bell Operating Companies (RBOC). All calls placed using their network will be billed by ITI and attached to local billing.

"Integretel is the billing agent for Intellicall's Intelliline system. All calls placed on this system will be billed by Integretel and attached to local billing. [This COCOT company] provides Intellicall with billing records from our phones. We retrieve these records, using our network of office computers, on a weekly basis. Intellicall then processes these records and the customer receives the bills on the Integretel portion of their bills.

"To reiterate, Intelliline Technology takes a Zero Plus dialed number and converts it to a One Plus number, storing the billing information within the phone for later retrieval."

Speaking of Intellicall, we were able to obtain a recent software release bulletin that detailed some of their payphones' features and bugs.

A new release was to have included a new FCC "pre" bong branding requirement. "Recent events, however, have led us to believe that a 'pre' bong brand may not be required, so the new speech file was not included."

What was included was "enhanced prompting" for more money. "Previously the phone requested coins for additional time 45 seconds before the current time period expired. This operation has been enhanced to time the prompting for additional coins depending on the amount of coins to be deposited. The larger the amount of money to be deposited, the longer the time." For amounts less than 50 cents, the phone will demand money 25 seconds before the time expires. For amounts higher than $3.50, the time is 70 seconds.

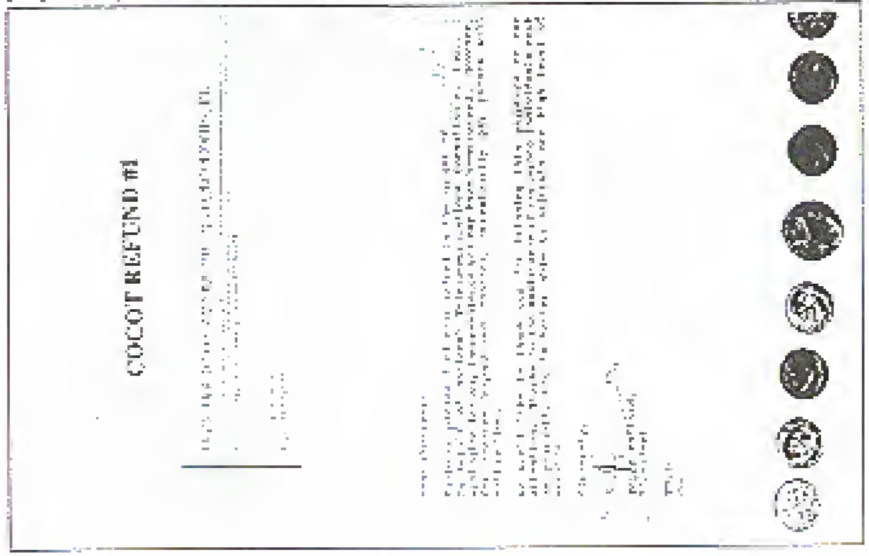
"Based on timing interactions between the patron dialing and the turbo VIC's outpulsing, some no connects to VIC's were occurring which resulted in the call going to the live operator. The new software has reduced the chances of this occurring.

"A problem has been found to occur when a certain set of events happen. It has been discovered that if an incoming call to the phone is answered by a patron, the call progresses for a few seconds, the caller hangs up, yet the called party stays off hook for approximately 10 seconds, then the phone has a chance of not detecting an on hook. There is also some dependency on the central office involved. The phone can only be brought out of this condition by cycling power. This condition has been resolved in the new version of software.

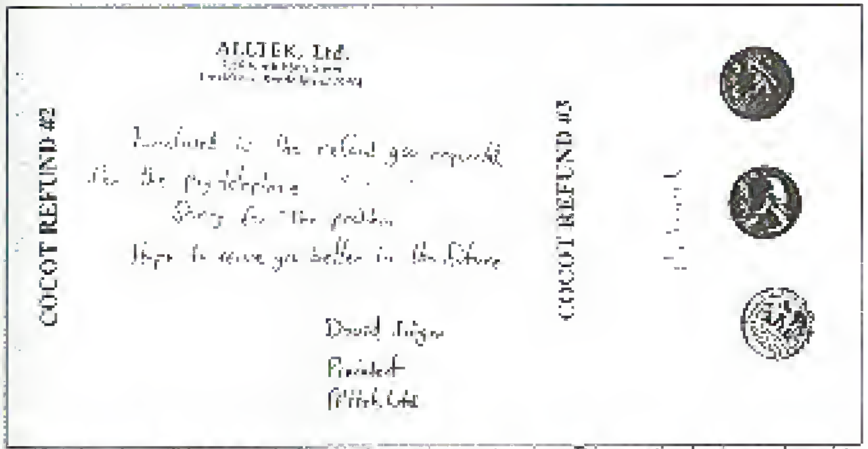
"An issue in previous versions was discovered dealing with 0+E*Z Collect calls in a Format I area. If an 0+E*Z Collect call was placed in a Format I area that also required all dialing to be 0+ ten digits, then an incorrect outpulsing of the direct dial number occurred.

"Several resolutions to issues with the IPServ are included in this release. These resolutions include removing some noise that was occurring during call initiation and E*Z Collect solicitation. Additionally, keyboard entry of several programmable fields (serial number, ANI, outcall number, etc.) has been made available for ease of installation.

"Previous versions of software could occasionally not detect SIT signaling if it occurred after ringbacks. This has been corrected in this new version of software."



COCOT REFUND #1



COCOT REFUND #2

ALLTEK, Ltd.

Enclosed is the refund you requested for the payphone

Sorry for the problem.

Hope to serve you better in the future

David Judge

President

Alltek Ltd.

COCOT REFUND #3

AN APPEAL FOR HELP

by Craig Neidorf

January 18-19, 1992 marked the two-year anniversary of my visit from and subsequent raid by the United States Secret Service, Southwestern Bell Security, and the University of Missouri Police Department.

The publicity and attention that once surrounded United States v. Craig Neidorf has long been over and, for most people involved, life has returned to normal.

Unfortunately things are not quite as simple for me.

After my trial concluded, I went back to school at the University of Missouri, and hit the books hard. I earned a 4.0 (straight A average) that semester, focusing on political science and pre-law courses. I did almost as well the following spring and summer semesters. I graduated on August 2, 1991.

However, my legal bills remained very high. In fact, my parents and I still owe close to $50,000.

I have always been uncomfortable with the idea of actually making a direct appeal to people to send donations in to my defense fund, but over the last year and a half, my idealism about the future has faded and been replaced with reality.

At the end of my trial, my legal fees totaled about $108,000 and this figure does not include travel expenses in going back and forth to Chicago from St. Louis and Columbia or any other related expenditures that I had to make during that seven month period.

This figure does not include the money I lost by having to drop most of my classes at the University of Missouri that semester because I could not consistently attend class during my ordeal.

This figure does not reflect the pain and suffering that my family and I were put through by a malicious and ignorant prosecutor and other similarly unpleasant people at Bellsouth, Illinois Bell, Bellcore, and AT&T.

This figure does not include the traumatic incidents of my suspension from the Zeta Beta Tau fraternity or the threats of expulsion I received from the Chancellor's office of the University of Missouri.

And finally this figure does not include the additional $900 I had to spend to finally get my arrest records expunged. That fee could and should have been avoided altogether except, as with the trial, William Cook (the assistant U.S. attorney) opposed my motion for expungement and so several more motions and court appearances were necessary for me to achieve victory.

The number one *myth* about my legal fees is that they were paid by the Electronic Frontier Foundation. This is complete fiction. Although I appeared to have been somewhat of a spokesperson and "poster-child" for the EFF throughout 1990 and 1991, and despite what you may have read anywhere else, there were no monetary contributions granted to me by that organization. *None.* There was a private and very generous donation made by Mitch Kapor personally, but this is separate from the EFF.

EFF did pay for some legal motions to be filed in my case regarding the First Amendment, but since these motions were denied, they impacted only slightly on the outcome of my trial. The most beneficial outcome of the EFF's involvement with my case was the general increase in awareness in the community at large to the issues my case presented.

More than a year has passed since the day my trial ended.

My entire life savings that I had stored for college and law school was needed as a downpayment on my legal fees and my parents of course had to give up most of their savings as well. A payment plan was arranged over what looks to be a ten year period. We had no choice but to accept that these were the cards life had dealt us and after all things could be much worse. I have my health and my freedom (such as it is) and these things are worth more than money.

However, I am a young person starting out in life. I have applied to several law schools across the country, both public and private. Unfortunately, after reviewing my financial options, I have discovered that the expense of a legal education may now place it very far beyond my means.

Like a very large number of Americans, the recession has hit home, putting my father out of work and keeping my mother in a job beneath her talents.

It seriously pains me to have to do this, but trust me when I tell you that I've thought about this for a long time. I need your help to get my legal bills paid. I need to be able to live my life without this debt hanging over my head. There are thousands of people who read 2600. If each person only contributed $20 it could wipe out this debt entirely. You see, helping me out is not beyond the reach of our community if we all work together. Consider it an investment in your future, because what happened to me can happen to anyone and with a legal education I'll be back to return the favor.

If you find that you can afford to help me, you have my most sincere thanks and appreciation. I know a lot of you are in tight financial situations like me and can sympathize with what I am going through. If you are unable to help me because you are having problems of your own then you have my sympathy as well.

Please make checks or money orders payable to: Katten, Muchin, & Zavis.

Send them to: Sheldon Zenner
Katten, Muchin, & Zavis 525 West
Monroe Street Suite 1600 Chicago,
Illinois 60606-3693.

Please don't forget to write my name in the memo section of the check or enclose a letter explaining what the check is for. If you don't do that, KMZ will not credit my account for the amount of the check.

I'd also appreciate any tips or leads on potential sources of financial aid, grants, and scholarships available for an aspiring law student.

You can reach Craig through 2600. Donations, anonymous or otherwise, can also be made through 2600 Neidorf Defense Fund, PO Box 99, Middle Island, NY 11953.

Hacker Beer

Common in Germany and Austria, we're told this could be translated as "Hacker Nutrient Beer."

what L.O.D. really stands for

THE LEGION OF DECENCY

Shortly after the close of the last war, Hollywood producers came out with a new "line" of pictures. This was comprised largely of pictures glorifying (1) "the American girl"; (2) gangsters and their philosophy. Not only was the producers' idea of the "American girl" repulsive to anyone with a sense of decency, but the quality of the pictures produced declined with this moral laxity. The rat-tat-tat machine gun of the cornered gangster did not produce any ennobling thoughts either; and the general result of the two themes was a poor level in quality for the average picture.

LEGION OF DECENCY ORGANIZED

The Legion of Decency was finally organized effectively and did a great deal of good. Hollywood magnates, confronted not with isolated protests, but with an organization composed of sworn members, realized their mistakes, and produced pictures of the type of "Goodbye, Mr. Chips" and "Windswept." Classics were dramatized and presented to the people through the attractive medium that the motion picture is. The quality of Hollywood pictures began to climb steadily.

SUPPORT THE LEGION

The Legion of Decency deserves our support. Even if we dismissed the serious moral question, we should support such an organization for the sake of our own entertainment. Lurid, indecent pictures do not edify; mud never cleans anything. The sentiments, theories, and actions portrayed in motion pictures must be morally good if we, who enjoy beauty, are to enjoy the pictures; for that which is good is true; and only that which is true is beautiful.

—C. M. W.

From a Catholic school's newspaper in the 1950's.

ANALYSIS: Gulf War Printer Virus

by Anonymous

I work closely with the technical aspects of the operating system on IBM mainframes so I followed with some interest the accounts of the "Gulf War Virus." (News organizations in January reported the story of a computer virus introduced into an Iraqi air defense system via a printer.) My first reaction was one of amazement that the National Security Agency had pulled off such a stunt. But when I thought about it further it began to seem less and less reasonable and more and more likely that the whole thing was a piece of "disinformation."

There are three ways that the printer might have been attached to the mainframe: (1) Channel attached. If it was channel-attached then there is virtually no way that it could initiate an action that would cause the modification of software on the mainframe. A printer is an *output* device. It can only tell the computer stuff like, "I finished printing a line," "I have a jam," etc. It does this through very simple codes. (2) Attached to a network or (3) attached remotely... (2) and (3) are similar in terms of requirements. If it were attached in one of these two ways then it is at least conceivable that, with an enormous effort, it could transform itself from a print-server into something capable of initiating input into the mainframe. This would involve a lot of "fooling the system." Once it had transformed itself it would have to fool the mainframe again into considering it a legitimate user who had the proper security to either initiate batch jobs or work interactively. Once it had done that it would have to know the name of the library where the CRT software resided and the name of the module that controlled the CRT's. It would have to convince the security system that it should be allowed to access this library. Once it had done that it could then make the very subtle change indicated in the article that would only go into effect under special circumstances. (A subtle change like that would be more difficult than a gross change that would, for example, simply bring down the entire system.) And, all of this incredible coding would, presumably, be done in the 1k or 2k that is available in a ROM chip!

Now consider what I think is more likely: First you have to ask yourself, "Why would the NSA tell this story? If they could really do something neat like this, why wouldn't they keep it a secret to use again in the future?" I can only imagine two reasons that they might tell such a story: (1) There is an Iraqi computer insider who they are trying to protect (the guy who really did the deed) by diverting attention. (2) The software (like most of the Iraqi equipment) probably came from a Western country. The company that created the CRT software might well have left a "logic bomb" in the software in case Saddam pulled a stunt like he pulled. The company probably does not want it to be known that they leave such bombs in their software, so the NSA wants, again, to protect them and divert attention.

I think that the disinformation theory gains some credibility from the information that is presented in the stories that are circulating. We are told almost nothing about the technical details but we are told *everything* about the printer. How it came in, where it came from, the approximate time frame, everything but the serial number. I suspect that when the Iraqis read the story and open up the printer there will probably be color-coded chips there stamped "NSA".

As if mainframe security people don't have enough to worry about, I imagine that for the next 20 years they will have to answer questions about the possibility of introducing a virus into the mainframe from the least likely source: a printer.

LETTERS: *(Continued from page 30)*

With this mod, the tones will always be 1721.0 Hz and 2208.1 Hz and the (incorrect) timing will always be 54.62 mS on and off. Even though two of these three parameters are at the very edge of the spec, they still work, but since DSP is often used, it would be much too easy to look for these exact frequencies and timing! If they (local Bell/AT&T) want you, they get you! Perhaps one payphone out of millions might find this clone (old frequency just right and Coca-Cola poured down the coin slot?). To avoid detection a free running 6.5 Mhz OSC would help, but a dialer with a separate controller would be necessary to bring the timing into the more nominal 35-40 mS. (The top of the line RS dialer had a separate processor and 5089 DTMF chip, and converting was a rather skilled operation, but 99 percent safe!) *This device is a bust!*

Billsf
Amsterdam

Reading Stripes

Dear 2600:

Oh, how it warms the cockles of my heart to see a good article on magnetic card technology. Magnetic heads are not hard to come by; something out of a tape recorder should do. A product called "KYREAD" is useful: you just put this liquid on a card's magnetic stripe, the iron powder in it settles on the magnetized areas while the alcohol it's suspended in evaporates, and presto! - you can see the stripes, often more than one or two carrying the info they tell you is on the card.

These cards and the little gray machines that you are seeing everywhere these days are going to become more and more important. We need to spread the word that these are relatively simple machines with the potential for a lot of good clean fun. I should know, I was relieved of duties at the birthplace of the gray boxes for indulging in some grins and giggles myself. I would love to help you in your pursuit of the little boxes' secrets, but I must admit, it's not hard to do, though. An Eprom copier is very useful here - that gives people the entire program, passwords and all. Use your imagination and Kamyland. Have fun!

Trigger
Santa Ana, CA

Lock Your Terminal

Dear 2600:

A smaller lock script than presented in the last issue. Type 'lock [password]' at your UNIX(tm) prompt, and away you go! The password 'secret' is hard coded in case you forget your password. Go ahead and take it out to keep people from reading your script to get the default password.

```
# @(#) Lock for UNIX(tm) Systems
trap "echo Dummy!! Calling the phone police!; stty
echo; kill $$" 2 15
PATH=/bin:/usr/bin
SECRET="secret"
stty -echo
echo "Lock string: \c"
read BUF1
echo
echo "Lock:terminal is SECURE. Enter password to
unlock."
while :
do BUF2=`line < /dev/tty` if [ "$BUF2" = "$BUF1" ]
] then break
elif [ "$BUF2" = "$SECRET" ]
then break
fi
echo "Please dont mess with this terminal...I will
return shortly."
done
stty echo
```

Crazy-Z Phreaker
Skunk Works

Russian Technology

Dear 2600:

Seen your magazine for the first time here. Very much impressed. Read it from the first to the last page non-stop. Tried several things with no success.

Do you know that:

Caller ID is a widely used thing in (ex) Soviet Union and ID detectors are available and anti-caller-ID devices are available as well? *Nobody* cares about the privacy.

I can now dial any country, as other people in Moscow also can for the first time ever. They allowed it for anybody but only from 0000 till 0800 local time. Sleepless night, as usual.

Telenet (Sprint) is the only packet switching net really *publicly* available here. But those numbers you've listed in the Summer 1991 volume refuse to collect connect.

The phone booth featured as a part of the backside is, in fact, a modern one. I'll try to take a picture of a much older version when I go to another city.

The Soviet phone system was designed by KGB people and has lots of interesting features inside. Like Caller ID, recording, tapping, access codes capable of breaking the conversation when an "important phone" calls long distance, etc. Everything's secret, but people have got to know.

The KGB is to sell its secret phone system, said to be secure, to businesses with big money in early 1992.

Accessing US can be done from here via Finland's USA Direct by AT&T. Any time, any phone.

I've got 120 kg of potatoes to feed a family.

I have those and other interesting bits of news from this neck of the woods.

In a related question, I'd like to ask if 2600 is available in electronic form? And have you any subscribers among Soviets? Can we get some copies?

KT
Moscow

We're not available electronically. And so far, we haven't penetrated the former Iron Curtain. At least, not so far as we can tell. But we are offering free subscriptions (for a limited time) to anyone in Eastern Europe and the former Soviet Union.

2600 marketplace

2600 MEETINGS. First Friday of the month at the Citicorp Center - from 5 to 8 pm in the lobby near the payphones. 153 E 53rd St., NY, between Lex & 3rd. Come by, drop off articles, ask questions, find the undercover agents. Call 516-751-2600 for more info. Payphone numbers at Citicorp: 212-223-9011, 212-223-8927, 212-308-8044, 212-308-8162. **Meetings also take place in San Francisco at 4 Embarcadero Plaza** (inside) starting at 5 pm Pacific Time on the first Friday of the month. Payphone numbers: 415 398 9803,4,5,6. You can start meetings in your own city! Let us know if you do.

AMIGA, IBM (in that order) hackware, war dialers, extender scanners, codebreakers, encryption software, disassemblers/assemblers, tone recognition programs, computer and phreaking hardware plans and schematics, and good books and articles (on hacking, cracking, phreaking, data encryption, general and military cryptography, coding and coding theory, mathematics, A.I., virtual reality, networking and telecommunications, viruses, programming and theory, electronics, physics, philosophy, linguistics, political science, etc.). Send info or disks to Stephen B., Simon's Rock College, Great Barrington, MA 01230.

AUTHOR looking for real-life war stories by hackers/phreaks etc. Anonymity if requested. Winn Schwartau, Inter-Pact Press, 3106 Knobview Dr., Nashville, TN 37214. (615) 883-6741, FAX (615) 883-6781.

FOR SALE: 451 viruses for the IBM on one 3.5" 1.44M disk. Several with source code and documentation. Send $10 to R. Jones, 21067 Jones Mill, Long Beach, MS 39560 or email me at RJones@USMCP6.BitNet. Supplied for educational purposes only.

LOW RUN NYC is seeking writers for its bimonthly aggressive newsletter. So if you believe in right vs. might, if you're raw, passionate, and pissed off at the same time, we want you to join us! All articles, letters, experiences, and suggestions should be sent to: Low Run, 37 Lexington Ave, #232, New York, NY 10010 (your telephone number is optional but would be useful for clarifications). All sources, if included, will be kept strictly confidential. Requests for issues should also be addressed to the above, along with a SSAME (Stamped Self Addressed Medium Envelope).

WANTED: Schematics and data kits for telephone line voice scramblers. Prefer digital units using DES encrypt/decrypt algorithm. Code key must be user changeable from exterior of unit. Please send price/details to A.G. Morris, PO Box 4652, Long Beach, CA 90804-4652.

SPY SHOP CATALOGUE: Packed with equipment, items, personal and privacy protection surveillance transmitters in kit form, telephone taps, bugs, stun guns, room monitors, decoding devices, analyzers, covert tracking systems, defense sprays, caller ID, people locators - find anyone anywhere! Detection systems, tap trap, voice changers, scramblers, secure phones, and much more. Send $5 check or money order to: Bug Busters, PO Box 978, Dept. 2-6, Smithtown, NY 11786. FAX 516-929-0372.

KNOW WHO'S CALLING! The Call Identifier has the answer. Displays caller's phone number when your phone rings. Stores phone numbers with date and time of call. $79.95. $10 off for 2600 subscribers. Surveillance-Countersurveillance equipment catalog $5. Miniature Surveillance Transmitter Kits $39.95 ppd. Voice changers, scramblers, vehicle tracking, bug and phone tap detectors, books, videos, etc. D.T.E., PO Box 337, Buffalo, NY 14226. (716) 691-3476.

THE LITTLE BLACK BOOK OF COMPUTER VIRUSES. The first book on how to write them! 190 pgs. soft cover, with full IBM PC source code. $14.95 postpaid, or ask your local bookstore to order it (ISBN 0-929408-02-0) American Eagle Publications, Box 41401, Tucson, AZ 85717.

TECHNICAL SURVEILLANCE COUNTER-MEASURES, communications engineering services. Ross Engineering, Inc., 7906 Hope Valley Court, Adamstown, MD 21710. 800 US DEBUG.

COCOTS FOR SALE: Perfect working condition, removed from service. Credit card only type, has card reader built into unit. DTMF, 12 number speed dial. $60 each plus $15 shipping. Call or write for info. Bill Rogers, 2030 E. Charleston Blvd., Las Vegas, NV 89104. 800 856 8501, (702) 382-7348.

TAP BACK ISSUES, complete set Vol 1-91 of QUALITY copies from originals. Includes schematics and indexes. $100 postpaid. Via UPS or First Class Mail. Copy of 1971 Esquire article "The Secrets of the Little Blue Box" $5 & large SASE w/52 cents of stamps. Pete G., PO Box 463, Mt. Laurel, NJ 08054. We are the Original!

Marketplace ads are free to subscribers! Send your ad to: 2600 Marketplace, PO Box 99, Middle Island, NY 11953. Include your address label. Ads may be edited or not printed at our discretion. Deadline for Spring issue: 4/15/92.

U.S. Phone Companies Face Built-In Privacy Hole

Phone companies across the nation are cracking down on hacker explorations in the world of Busy Line Verification (BLV). By exploiting a weakness, it's possible to remotely listen in on phone conversations at a selected telephone number. While the phone companies can do this any time they want, this recently discovered self-serve monitoring feature has created a telco crisis of sorts.

According to an internal Bellcore memo from 1991 and Bell Operating Company documents, a "significant and sophisticated vulnerability" exists that could affect the security and privacy of BLV. In addition, networks using a DMS-TOPS architecture are affected.

> *"There is no proof that the hacker community knows about the vulnerability."*

According to this and other documents circulating within the Bell Operating Companies, an intruder who gains access to an OA&M port in an office that has a BLV trunk group and who is able to bypass port security and get "access to the switch at a craft shell level" would be able to exploit this vulnerability.

The intruder can listen in on phone calls by following these four steps:

"1. *Query the switch to determine the Routing Class Code assigned to the BLV trunk group.*

"2. *Find a vacant telephone number served by that switch.*

"3. *Via recent change, assign the Routing Class Code of the BLV trunks to the Chart Column value of the DN (directory number) of the vacant telephone number.*

"4. *Add call forwarding to the vacant telephone number (Remote Call Forwarding would allow remote definition of the target telephone number while Call Forwarding Fixed would only allow the specification of one target per recent change message or vacant line).*"

By calling the vacant phone number, the intruder would get routed to the BLV trunk group and would then be connected on a "no-test vertical" to the target phone line in a bridged connection.

According to one of the documents, there is no proof that the hacker community knows about the vulnerability. The authors did express great concern over the publication of an article entitled "Central Office Operations — The End Office Environment" which appeared in the electronic newsletter *Legion of Doom/Hackers Technical Journal*. In this article, reference is made to the "No Test Trunk."

The article says, "All of these testing systems have one thing in common: they access the line through a No Test Trunk. This is a switch which can drop in on a specific path or line and connect it to the testing device. It depends on the device connected to the trunk, but there is usually a noticeable click heard on the tested line when the No Test Trunk drops in. Also, the testing devices I have mentioned here will seize the line, busying it out. This will present problems when trying to monitor calls, as you would have to drop in during the call. The No Test Trunk is also the method in which operator consoles perform verifications and interrupts."

In order to track down people who might be abusing this security hole, phone companies across the nation are being advised to perform the following four steps:

"1. *Refer to Chart Columns (or equivalent feature tables) and validate their integrity by checking against the corresponding office records.*

"2. *Execute an appropriate command to extract the directory numbers to which features such as BLV and Call Forwarding have been assigned.*

"3. *Extract the information on the directory number(s) from where the codes relating to BLV and Call Forwarding were assigned to vacant directory numbers.*

"4. *Take appropriate action including on-line evidence gathering, if warranted.*"

Since there are different vendors (OSPS from AT&T, TOPS from NTI, etc.) as well as different phone companies, each with their own architecture, the problem cannot go away overnight.

And even if hackers are denied access to this "feature", BLV networks will still have the capability of being used to monitor phone lines. Who will be monitored and who will be listening are two forever unanswered questions.

These kits, designed by Billsf, originally appeared in Hack-Tic, the Dutch hacker magazine.

FM Wireless Transmitter

We at 2600 tested this wireless FM transmitter thoroughly, and can safely say that it is well worth your time and effort to build. Most FM transmitters claim ranges of up to a mile. While this may be true, we often find the maximum range to be far less than expected. We used two fresh alkaline 9-volt batteries and were able to overpower other FM stations from up to 300 feet. Although this may not sound impressive, it is when you consider that we were competing with powerful FM stations putting out up to 50,000 watts. The transmitter can reach much further when it does not have to compete with other stations. It will also work better if it is used outdoors in a high place.

Although this transmitter can be used as a "bug," we have found a much better use for it. Find a supermarket that is playing an FM radio over a loudspeaker. In all likelihood, your taste in music will differ from those who own the supermarket. Use the transmitter to overpower the existing station and transmit your own music. You can easily modify the device to accept the audio output of a portable tape playing device.

The transmitter has a power of 25 mW and can be adjusted from 80 to 130 MHz by slowly turning the screw on C3 (4-40 pF). If you wish to change the frequency outside these limits, the rule is: twice as many windings on the coil will cut the frequency in half. By upping the battery voltage to 12 or 15 Volts, the transmitting power is also raised. The power supply has to be very well stabilized so it is best to use batteries instead of a transformer. Never connect more than 18 Volts if you care about your transistors.

Expect to take at least an hour building the transmitter. You will want to construct the device on a small breadboard. Do not use a soldering iron of more than 30 Watts. Your best bet is to purchase a soldering iron with a pencil-thin tip. Make sure that the two transistors and C1 (10 uF) are facing the right way. The coil is extremely important. Wrap shielded, unbraided wire 6 3/4 turns around a cylindrical object approximately 3 mm in diameter. A 1/8" drill bit will suit the purpose. The piece of wire shown in the diagram is your antenna and should be approximately 69 cm long. Use a flexible, shielded piece of wire and remember that the antenna will ultimately determine how far the device transmits.

Do not even think about going to Radio Shack to purchase your supplies. First of all, Radio Shack does not carry all of the parts that you will need. Although you could substitute similar transistors for the ones that are used, keep in mind that the circuit was specially designed to work at optimum efficiency with the parts used. Secondly, Radio Shack uses inferior parts and will overcharge you. We know that you probably want to start construction right away, and Radio Shack may be the closest and most convenient supply of electronic parts, but you will be wasting your time and money if you go there. If you are serious about building the device, then be patient and order the parts from electronics firms listed in the back of *Popular Electronics* or similar magazines. Order at least two of everything so that you will have spares in case you mess up.

Parts List

Resistors	Values	Colors
R1	10 kOhm	brown, black, orange, gold
R2	4.7 kOhm	yellow, violet, red, gold
R3	33 kOhm	orange, orange, orange, gold
R4	120 kOhm	brown, red, brown, gold

Capacitors	Values	Notes
C1	10 uF	polarized electrolytic capacitor
C2	1.0 nF	
C3	4-40 pF	tuning capacitor
C4	10 pF	
C5	3.3 pF	
C6	10 nF	
C7	22 pF	
C8	1.0 nF	

Transistors	Type	Industry name
Q1	NPN	BC547B
Q2	NPN	BF241

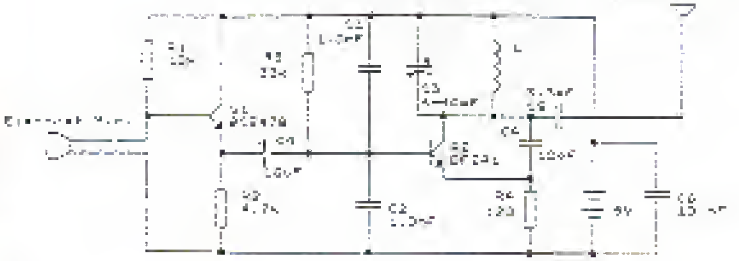
Electric Microphone

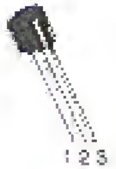
Coil: shielded, unbraided 1 mm wire coiled 6 3/4 times on a 3 mm "air core".

Antenna: flexible and shielded, 69 cm long.

Battery snap(s)

Breadboard: the smaller the better!





BC557B, BC547B
1=C, 2=B, 3=E

BF241
1=C, 2=E 3=B

FM Telephone Transmitter

The FM telephone transmitter is essentially the same circuit as the FM wireless transmitter except that it is modified to take its input and power from a telephone line. The transmitter has a power of about 5 mW, somewhat less than its sister transmitter. The LEDs are there to stabilize the power; they're not just there for show. The device also uses a full-wave rectifier so that you do not have to worry about polarity when you connect it to a telephone line. Once the transmitter is in place, it will only transmit when the receiver is lifted.

Parts List

Resistors	Values	Colors
R1	47 kOhm	yellow, violet, orange, gold
R2	1 MOhm	brown, black, green, gold
R3	47 kOhm	yellow, violet, orange, gold
R4	4.7 kOhm	yellow, violet, red, gold
R5	100 kOhm	brown, black, yellow, gold
R6	33 kOhm	orange, orange, orange, gold
R7	120 kOhm	brown, red, brown, gold

Capacitors	Values	Notes
C1	10 nF	
C2	1.0 nF	
C3	1.0 nF	
C4	4-40 pF	tuning capacitor
C5	10 pF	
C6	3.3 pF	
C7	22 pF	

Diodes	Industry name
D1	1N4148
D2	1N4148
D3	1N4148
D4	1N4148
D5	small LED
D6	small LED

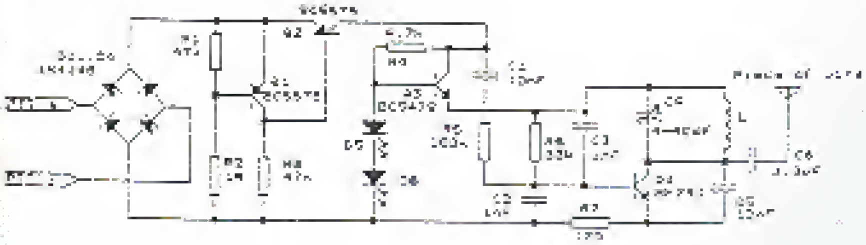
Transistors	Type	Industry name
Q1	PNP	BC557B
Q2	PNP	BC557B
Q3	NPN	BC547B
Q4	NPN	BF241

Coil: shielded, unbraided wire coiled 6 3/4 times on a 3 mm "air core".

Antenna: flexible and shielded, 69 cm long.

Alligator clips: to attach the device to the telephone line.

Breadboard: the smaller the better!



Human Database Centers

by PW

UCC Network: 185-A Commerce Circle. Sacramento, CA 95815. (916)929-4311

Data Check: PO Box 922169, Sylmar, CA 91392. (818) 783-DATA, (818) 367-0154, (818)903-1617

J. Dillon Ross & Company: PO Box 539, Pauma Valley, CA 92061. (619) 742-4273 (computer)

Super Bureau Incorporated: 2600 Garden Road West 224, Monterey, CA 93940. 800-541-6821. (408) 372-6624 (fax)

California Municipal Criminal Court Records: 800-332-7999, 800-365-2667 (computer) (71E, 1200/2400, CISDEMO)

Automated Name Index: PO Box 813, Glendale. CA 91209; 5113 Lankershim Blvd., North Hollywood. CA 91601. (818) 506-1957, (818) 980-1079 (fax)

Search Unlimited: 18030 Sky Park Circle. Suite 205, Irvine. CA 92714. (714) 474-1916, (714) 474-9739 (fax)

Court Record Consultants: 17029 Devonshire St., Suite 166, Northridge, CA 91325. (818) 366-1906, (818) 366-1985 (fax)

The Source: PO Box 88, Cookeville, TN 38503. 800-678-8774, (615) 528-1986 (fax), 73330,2743 (Compuserve)

Data Search: 3600 American River Drive, Sacramento, CA 95864. (916) 485-3282

Intelligence Network Incorporated: PO Box 727, Clearwater, FL 34617. (813) 449-0072, 800-562-4007, (813) 448-0949 (fax)

APscreen (bank account searches): 2043 Westcliff Dr., Suite 300, Newport Beach, CA 92660. (714) 646-4003, (714) 646-5160 (fax)

Atlantic International Associates: (207) 761-5974, (207) 761-0834 (fax)

National Information Resource Service: PO Box 1021, Jackson, MI 49204. (517) 783 4545

Locate Unlimited: 800-365-5622, (602) 990-7146

DataQuick (real estate): 13160 Mindanao Way, Suite 240, Marina Del Rey, CA 90292. (213) 306-4295

AA Credit Information Services: 4419 Cowan Road, Suite 201A, Tucker, GA 30084. (404) 621-0151, (404) 621-0142

Farmer & Associates: 16845 N. 29th Ave., Suite 1205, Phoenix, AZ 85023. (602) 843-5236, (602) 938-2688 (fax)

DataFax (National Association of Investigative Specialists Incorporated): (512) 832-0355, (512) 832-9376 (fax), 76050.3601 (Compuserve)

CDB Infotek: 701 S. Parker Ave., Suite 4500, Orange, CA 92668. (714) 542-2727

DataTrac: PO Box 703, Port Coquitlam, B.C., V3B 6H9, Canada. (604) 469-0114, (604) 469-9609 (fax)

Trans Union Credit Info: 1561 E. Orangethorpe Ave., Fullerton, CA 92631. (213) 620-1355

2600 NEEDS WRITERS!

Send us your articles written from the hacker perspective. If we print it, you'll get a free subscription! But more importantly, you'll be helping to share the information that others want to keep secret.

Send articles to:
2600 Article Submission
PO Box 99
Middle Island, NY 11953
Internet: 2600@well.sf.ca.us

RESPECT YOUR LABEL

IF YOUR ADDRESS LABEL SAYS IT'S TIME TO RENEW, YOU SHOULD TAKE IT VERY SERIOUSLY. UNLIKE MOST OTHER PUBLICATIONS, WE WON'T SEND YOU A BUNCH OF REMINDERS OVER AND OVER AGAIN. WE DON'T BELIEVE IN HOUNDING OUR (FORMER) READERS. SO YOU COULD FIND YOURSELF WONDERING WHY YOU HAVEN'T SEEN 2600 IN THE LAST FEW MONTHS. UNFORTUNATELY, WHEN THIS HAPPENS, SUBSCRIBERS USUALLY MISS AN ISSUE BY THE TIME THEY FIGURE OUT WHAT'S HAPPENED. AND IF YOU'VE EVER MISSED AN ISSUE OF 2600, YOU KNOW WHAT THAT ENTAILS. DON'T GET CAUGHT SHORT. RENEW BEFORE YOUR LAST ISSUE ARRIVES SO THERE WON'T BE ANY GAPS. RENEW FOR MULTIPLE YEARS SO YOU WON'T HAVE TO WORRY ABOUT THIS QUITE SO OFTEN. AND FOR YOU CORPORATIONS AND INSTITUTIONS THAT TAKE FOREVER TO PROCESS PURCHASE ORDERS, CONSIDER A LIFETIME SUBSCRIPTION SO YOU'LL NEVER HAVE TO DEAL WITH ANY OF THIS AGAIN.

INDIVIDUAL SUBSCRIPTION

□ 1 year/$21 □ 2 years/$38 □ 3 years/$54

CORPORATE SUBSCRIPTION

□ 1 year/$50 □ 2 years/$90 □ 3 years/$125

OVERSEAS SUBSCRIPTION

□ 1 year, individual/$30 □ 1 year, corporate/$65

LIFETIME SUBSCRIPTION

□ $260 (the dire threats on this page will never apply to you)

BACK ISSUES (invaluable reference material)

□ 1984/$25 □ 1985/$25 □ 1986/$25 □ 1987/$25

□ 1988/$25 □ 1989/$25 □ 1990/$25

(OVERSEAS: ADD $5 PER YEAR OF BACK ISSUES)

(individual back issues for 1988,1989, 1990 are $6.25 each, $7.50 overseas)

TOTAL AMOUNT ENCLOSED: □